PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-289297
(43)Date of publication of application : 10.10.2003

(51)Int.Cl. H04L 9/08

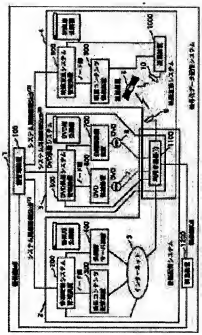
(21)Application number : 2003-014027
(22)Date of filing : 22.01.2003

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : MATSUZAKI NATSUME
NAKANO TOSHIHISA
MATSUMOTO TSUTOMU

(30)Priority
Priority number : 2002016547 Priority date : 25.01.2002 Priority country : JP

(54) DATA DISTRIBUTION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To enable each of content supply system to use a group key management method employing flexible and unique structures, when a single user apparatus is connected a plurality of content supply systems.
SOLUTION: A manager of each content supply system uses a system apparatus key, distributed from a key management organization to generate a public list corresponding to a unique tree structure, and discloses the list, when the content supply system is constructed. The user apparatus stores only the apparatus key, corresponding to a leaf of the tree structure. Using the public list which is disclosed via a web site or package media, the user apparatus constructs the tree structure sequentially from the bottom to the top, and derives a node key corresponding to the user apparatus. Next, the user apparatus decrypts an encrypted content by using the node key.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－289297
（P2003－289297Ａ）
(43)公開日　平成15年10月10日(2003.10.10)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｂ	５Ｊ１０４
			６０１Ｅ	
			６０１Ａ	

審査請求　未請求　請求項の数40　ＯＬ　（全 58 頁）

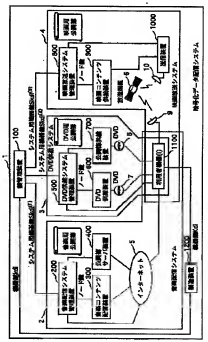
(21)出願番号　特願2003－14027(P2003－14027)
(22)出願日　平成15年１月22日(2003.1.22)
(31)優先権主張番号　特願2002－16547(P2002－16547)
(32)優先日　平成14年１月25日(2002.1.25)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　松崎　なつめ
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　中野　稔久
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100090446
弁理士　中島　司朗

最終頁に続く

(54)【発明の名称】　データ配信システム

(57)【要約】
【課題】１個の利用者機器が複数のコンテンツ供給システムに接続される場合に、それぞれのコンテンツ供給システムが柔軟で独自の木構造を用いたグループ鍵管理方法を使用することできるようにする。
【解決手段】コンテンツ供給システムの管理者は、鍵管理機関より配布されたシステム用の機器鍵を用いて、独自の木構造に対応する公開簿を生成し、システム構築時に公開する。利用者機器は、木構造のリーフに対応した機器鍵だけを保持する。Webページやパッケージメディアを介して公開された公開簿を用いて、利用者機器は、下から上に順次木構造を構築し、対応するノード鍵を求める。次に、ノード鍵を用いて暗号化コンテンツを復号する。



1

【特許請求の範囲】

【請求項１】　鍵管理装置と複数のコンテンツ供給装置と１個以上の利用者機器とから構成されるデータ配信システムであって、各コンテンツ供給装置は、それぞれ暗号化コンテンツを供給し、各利用者機器は、暗号化コンテンツを復号して利用し、

各利用者機器へ当該利用者機器に固有の機器鍵を出力し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第１システム用機器鍵を生成し、生成した前記第１システム用機器鍵を当該コンテンツ供給装置へ出力する鍵管理装置と、

それぞれ、前記第１システム用機器鍵を受け取り、受け取った前記第１システム用機器鍵に基づいて、デジタル著作物であるコンテンツを暗号化して暗号化コンテンツを生成し、生成した前記暗号化コンテンツを利用者機器へ出力する複数のコンテンツ供給装置と、

それぞれ、前記機器鍵を受け取り、前記暗号化コンテンツを受け取り、前記機器鍵及び前記コンテンツ供給装置に固有のシステム情報に基づいて前記一方向性関数を用いて前記利用者機器に固有の第２システム用機器鍵を生成し、生成した前記第２システム用機器鍵に基づいて、受け取った前記暗号化コンテンツを復号して復号コンテンツを生成する１個以上の利用者機器とから構成されることを特徴とするデータ配信システム。

【請求項２】　鍵管理装置と複数のコンテンツ供給装置と１個の利用者機器とから構成されるデータ配信システムであって、各コンテンツ供給装置は、それぞれ暗号化コンテンツを供給し、前記利用者機器は、暗号化コンテンツを復号して利用し、

前記利用者機器へ当該利用者機器に固有の機器鍵を出力し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第１システム用機器鍵を生成し、生成した前記第１システム用機器鍵を当該コンテンツ供給装置へ出力する鍵管理装置と、

それぞれ、前記第１システム用機器鍵を受け取り、前記第１システム用機器鍵に基づいて、コンテンツを暗号化する際に基づくデバイス鍵を決定し、決定した前記デバイス鍵に基づいて、デジタル著作物であるコンテンツを暗号化して暗号化コンテンツを生成し、前記暗号化コンテンツを前記利用者機器へ出力し、前記第１システム用機器鍵に基づいて、前記デバイス鍵を特定するための公開簿を生成し、生成した前記公開簿を公開する複数のコンテンツ供給装置と、

それぞれ、前記機器鍵を受け取り、前記暗号化コンテンツを受け取り、公開された前記公開簿を取得し、前記機器鍵及び前記コンテンツ供給装置に固有のシステム情報

2

に基づいて前記一方向性関数を用いて前記利用者機器に固有の第２システム用機器鍵を生成し、前記第２システム用機器鍵に基づいて、前記公開簿から前記デバイス鍵を特定し、特定した前記デバイス鍵に基づいて、受け取った前記暗号化コンテンツを復号して復号コンテンツを生成する１個の利用者機器とから構成されることを特徴とするデータ配信システム。

【請求項３】　前記コンテンツ供給装置は、前記第１システム用機器鍵がリーフに割り当てられ、他のノードにノード鍵が割り当てられた木構造を備え、前記木構造を用いて管理されている１個以上のノード鍵の中から前記デバイス鍵を決定し、前記デバイス鍵を用いて前記公開簿を生成し、

前記利用者機器は、前記木構造を用いて、前記公開簿から、前記デバイス鍵を特定することを特徴とする請求項２に記載のデータ配信システム。

【請求項４】　前記コンテンツ供給装置は、生成した前記公開簿を、Ｗｅｂサーバ、パッケージメディア又は放送メディアを介して、公開し、

前記利用者機器は、Ｗｅｂサーバ、パッケージメディア又は放送メディアを介して、前記公開簿を取得することを特徴とする請求項３に記載のデータ配信システム。

【請求項５】　前記コンテンツ供給装置は、前記公開簿のうち、前記利用者機器に関連する情報のみを出力し、前記利用者機器は、前記公開簿のうち、前記利用者機器に関連する情報のみを取得することを特徴とする請求項４に記載のデータ配信システム。

【請求項６】　鍵管理装置と複数のコンテンツ供給装置と１個の利用者機器とから構成されるデータ配信システムにおいて、前記鍵管理装置は、前記利用者機器へ当該利用者機器に固有の機器鍵を供給し、各コンテンツ供給装置は、それぞれ暗号化コンテンツを供給し、前記利用者機器は、暗号化コンテンツを復号して利用し、

前記利用者機器へ当該利用者機器に固有の機器鍵を出力する機器鍵出力手段と、

各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第１システム用機器鍵を生成し、生成した第１システム用機器鍵を前記コンテンツ供給装置へ出力するシステム用機器鍵生成手段とを備えることを特徴とする鍵管理装置。

【請求項７】　鍵管理装置と複数のコンテンツ供給装置と１個の利用者機器とから構成されるデータ配信システムにおける前記コンテンツ供給装置であって、前記鍵管理装置は、前記利用者機器へ当該利用者機器に固有の機器鍵を出力し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第１システム用機器鍵を生成し、生成した前記第１システム用機器鍵を当該コンテンツ供給装置へ出力し、

デジタル著作物であるコンテンツを記憶している記憶手段と、
前記鍵管理装置から前記第１システム用機器鍵を取得する取得手段と、
前記第１システム用機器鍵に基づいて、前記コンテンツを暗号化して暗号化コンテンツを生成する暗号手段と、
生成した前記暗号化コンテンツを利用者機器へ出力する出力手段とを備えることを特徴とするコンテンツ供給装置。

【請求項８】　鍵管理装置と複数のコンテンツ供給装置と１個の利用者機器とから構成されるデータ配信システムにおける前記コンテンツ供給装置であって、前記鍵管理装置は、前記利用者機器へ当該利用者機器に固有の機器鍵を出力し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第１システム用機器鍵を生成し、生成した前記第１システム用機器鍵を当該コンテンツ供給装置へ出力し、
デジタル著作物であるコンテンツを配憶している記憶手段と、
前記鍵管理装置から前記第１システム用機器鍵を取得する取得手段と、
前記第１システム用機器鍵に基づいて、コンテンツを暗号化する際に基づくデバイス鍵を決定し、決定した前記デバイス鍵に基づいて、前記コンテンツを暗号化して暗号化コンテンツを生成する暗号手段と、
前記第１システム用機器鍵に基づいて、前記デバイス鍵を特定するための公開簿を生成する公開簿生成手段と、
生成した前記公開簿を公開し、生成した前記暗号化コンテンツを利用者機器へ出力する出力手段とを備えることを特徴とするコンテンツ供給装置。

【請求項９】　前記出力手段は、生成した前記公開簿を、Ｗｅｂサーバ、パッケージメディア又は放送メディアを介して、公開することを特徴とする請求項８に記載のコンテンツ供給装置。

【請求項１０】　前記公開簿生成手段は、前記公開簿のうち、前記利用者機器に関連する利用者機器関連情報のみを生成し、
前記出力手段は、前記利用者機器関連情報を、公開することを特徴とする請求項９に記載のコンテンツ供給装置。

【請求項１１】　前記暗号手段は、前記第１システム用機器鍵がリーフに割り当てられ、他のノードにノード鍵が割り当てられた木構造を備え、前記木構造を用いて管理されている１個以上のノード鍵の中から前記デバイス鍵を決定することを特徴とする請求項８に記載のコンテンツ供給装置。

【請求項１２】　前記公開簿生成手段は、前記木構造のリーフを除く各ノードについて、当該ノードに割り当てられたノード鍵を、当該ノードの子ノードに割り当てられたノード鍵を用いて暗号化して暗号化ノード鍵を生成し、生成した暗号化ノード鍵を含む前記公開簿を生成することを特徴とする請求項１１に記載のコンテンツ供給装置。

【請求項１３】　前記公開簿生成手段は、前記木構造のリーフを除く各ノードについて、（ａ）当該ノードの１個の子ノードに割り当てられたノード鍵に一方向性関数を施して、当該ノードのノード鍵を生成し、（ｂ）当該ノードの別の子ノードに割り当てられたノード鍵を用いて、生成した当該ノードのノード鍵を暗号化して暗号化ノード鍵を生成し、（ｃ）生成した暗号化ノード鍵を含む前記公開簿を生成することを特徴とする請求項１１に記載のコンテンツ供給装置。

【請求項１４】　ｋを２以上の整数とし、ｍを０以上の整数とし、前記木構造をｋ分木とし、各ノード鍵を
（ｘ，ｙ）平面上の点とみなし、
前記公開簿生成手段は、（ｘ，ｙ）平面上において、共通の親ノードを持つｋ個の全てのノードのノード鍵を結ぶ（ｋ＋ｍ－１）次の曲線を生成し、前記曲線上のノード鍵以外の（ｋ＋ｍ－１）個の点を含む前記公開簿を生成することを特徴とする請求項１１に記載のコンテンツ供給装置。

【請求項１５】　前記公開簿生成手段は、前記（ｋ＋ｍ－１）次の曲線から一方向性関数を用いて予め決められた手法により一意に定まる点を、共通の親ノードに対応するノード鍵とすることを特徴とする請求項１４に記載のコンテンツ供給装置。

【請求項１６】　前記公開簿生成手段は、（ａ）公開鍵暗号の秘密鍵と公開鍵のペアを生成し、（ｂ）生成した前記秘密鍵を秘密に保持し、生成した前記公開鍵を含む前記公開簿を生成し、（ｃ）前記木構造のリーフを除くノードについて、当該ノードに対応するノード鍵に基づいて、前記秘密鍵を用いて暗号化して暗号化ノード鍵を生成し、生成した暗号化ノード鍵を、当該ノードの子ノードに対応するノード鍵とし、
前記出力手段は、前記公開簿を公開することを特徴とする請求項１１に記載のコンテンツ供給装置。

【請求項１７】　前記公開簿生成手段は、（ａ）秘密の素数ｐとｑの積ｎを計算し、（ｂ）ｐ－１とｑ－１の最小公倍数Ｌを求め、（ｃ）ｎと互いに素となるＬ以下の任意の整数ｅを求め、（ｄ）Ｌを法とするｅの逆元ｄを求めてこれを秘密鍵とし、（ｅ）前記整数ｅ及び前記積ｎを含む前記公開簿を生成し、（ｆ）前記ノードに対応するノード鍵と、当該ノードからその子ノードに接続する各パスに予め定められている個別のパス情報との排他的論理和を求め、（ｇ）排他的論理和を、前記秘密鍵ｄを用いて暗号化して暗号化ノード鍵を生成し、（ｈ）生成した暗号化ノード鍵を当該パスに接続する子ノードに対応するノード鍵とすることを特徴とする請求項１６に記載のコンテンツ供給装置。

5　　6

【請求項１８】　前記公開簿生成手段は、
（Ａ）木構造のリーフとそのすぐ上位のノードの間に関しては、
（ａ）前記木構造のリーフのすぐ上位の各ノードについて、当該ノードに割り当てられたノード鍵を、当該ノードの子ノードに割り当てられたノード鍵を用いて暗号化して暗号化ノード鍵を生成し、生成した暗号化ノード鍵を含む前記公開簿を生成し、又は（ｂ）木構造のリーフのすぐ上位の各ノードについて、当該ノードの１個の子ノードに割り当てられたノード鍵に一方向性関数を施して、当該ノードのノード鍵を生成し、当該ノードの別の子ノードに割り当てられたノード鍵を用いて、生成した当該ノードのノード鍵を暗号化して暗号化ノード鍵を生成し、生成した暗号化ノード鍵を含む前記公開簿を生成し、又は（ｃ）ｋを２以上の整数とし、ｍを０以上の整数とし、前記木構造をｋ分木とし、各ノード鍵を（ｘ，ｙ）平面上の点とみなし、（ｘ，ｙ）平面上において、共通の頂ノードを持つｋ個の全てのリーフのノード鍵を結ぶ（ｋ＋ｍ－１）次の曲線を生成し、前記曲線上のノード鍵以外の（ｋ＋ｍ－１）個の点を含む前記公開簿を生成し、
（Ｂ）上記以外のノードの間に関しては、公開鍵暗号の秘密鍵と公開鍵のペアを生成し、生成した前記秘密鍵を秘密に保持し、生成した前記公開鍵を含む前記公開簿を生成し、前記木構造のリーフ及びすぐ上位のノードを除くノードについて、当該ノードに対応するノード鍵に基づいて、前記秘密鍵を用いて暗号化して暗号化ノード鍵を生成し、生成した暗号化ノード鍵を、当該ノードの子ノードに対応するノード鍵とすることを特徴とする請求項１１に記載のコンテンツ供給装置。
【請求項１９】　鍵管理装置と複数のコンテンツ供給装置と１個の利用者機器とから構成されるデータ配信システムにおける前記利用者機器であって、前記鍵管理装置は、前記利用者機器へ当該利用者機器に固有の機器鍵を出力し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第１システム用機器鍵を生成し、生成した前記第１システム用機器鍵を当該コンテンツ供給装置へ出力し、各コンテンツ供給装置は、前記第１システム用機器鍵を受け取り、受け取った前記第１システム用機器鍵に基づいて、デジタル著作物であるコンテンツを暗号化して暗号化コンテンツを生成し、生成した前記暗号化コンテンツを利用者機器へ出力し、
前記鍵管理装置から前記機器鍵を受け取る取得手段と、
前記コンテンツ供給装置から前記暗号化コンテンツを受け取る受信手段と、
前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて前記一方向性関数を用いて前記利用者機器に固有の第２システム用機器鍵を生成するシステム用機器鍵生成手段と、
生成した第２システム用機器鍵に基づいて、受け取った前記暗号化コンテンツを復号して復号コンテンツを生成する復号手段とを備えることを特徴とする利用者機器。
【請求項２０】　鍵管理装置と複数のコンテンツ供給装置と１個の利用者機器とから構成されるデータ配信システムにおける前記利用者機器であって、前記鍵管理装置は、前記利用者機器へ当該利用者機器に固有の機器鍵を出力し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第１システム用機器鍵を生成し、生成した前記第１システム用機器鍵を当該コンテンツ供給装置へ出力し、各コンテンツ供給装置は、前記第１システム用機器鍵を受け取り、前記第１システム用機器鍵に基づいて、コンテンツを暗号化する際に基づくデバイス鍵を決定し、決定した前記デバイス鍵に基づいて、デジタル著作物であるコンテンツを暗号化して暗号化コンテンツを生成し、前記暗号化コンテンツを前記利用者機器へ出力し、前記第１システム用機器鍵に基づいて、前記デバイス鍵を特定するための公開簿を生成し、生成した前記公開簿を公開し、前記鍵管理装置から前記機器鍵を受け取り、公開された前記公開簿を取得し、前記コンテンツ供給装置から前記暗号化コンテンツを受け取る取得手段と、
前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて前記一方向性関数を用いて前記利用者機器に固有の第２システム用機器鍵を生成するシステム用機器鍵生成手段と、
前記第２システム用機器鍵に基づいて、前記公開簿から前記デバイス鍵を特定するデバイス鍵特定手段と、
特定した前記デバイス鍵に基づいて、受け取った前記暗号化コンテンツを復号して復号コンテンツを生成する復号手段とを備えることを特徴とする利用者機器。
【請求項２１】　前記コンテンツ供給装置は、生成した前記公開簿を、Ｗｅｂサーバ、パッケージメディア又は放送メディアを介して、公開し、
前記取得手段は、Ｗｅｂサーバ、パッケージメディア又は放送メディアを介して、前記公開簿を取得することを特徴とする請求項２０に記載の利用者機器。
【請求項２２】　前記コンテンツ供給装置は、前記公開簿のうち、前記利用者機器に関連する利用者機器関連情報のみを生成して公開し、
前記取得手段は、前記利用者機器関連情報を取得し、
前記デバイス鍵特定手段は、取得した前記利用者機器関連情報から当該利用者機器に対応する前記デバイス鍵を特定することを特徴とする請求項２１に記載の利用者機器。
【請求項２３】　前記コンテンツ供給装置は、前記第１システム用機器鍵がリーフに割り当てられ、他のノードにノード鍵が割り当てられた木構造を備え、前記木構造

を用いて管理されている１個以上のノード鍵の中から前記デバイス鍵を決定し、前記デバイス鍵を用いて前記公開簿を生成し、

前記デバイス鍵特定手段は、前記木構造を用いて、前記公開簿から、前記デバイス鍵を特定することを特徴とする請求項２０に記載の利用者機器。

【請求項２４】　前記デバイス鍵特定手段は、取得した前記公開簿を用いて、前記木構造において、あるリーフに割り当てられた第２システム用機器鍵から、当該リーフからルートに至る経路上の各ノードに対応するノード鍵を順次求めることを特徴とする請求項２３に記載の利用者機器。

【請求項２５】　前記コンテンツ供給装置は、前記木構造のリーフを除く各ノードについて、当該ノードに割り当てられたノード鍵を、当該ノードの子ノードに割り当てられたノード鍵を用いて暗号化して暗号化ノード鍵を生成し、生成した暗号化ノード鍵を含む前記公開簿を生成し、

前記デバイス鍵特定手段は、前記木構造の１個のノードに対応するノード鍵を用いて、取得した前記公開簿内の暗号化ノード鍵を復号して、当該ノードの親ノードのノード鍵を求めることを特徴とする請求項２４に記載の利用者機器。

【請求項２６】　前記コンテンツ供給装置は、前記木構造のリーフを除く各ノードについて、（ａ）当該ノードの１個の子ノードに割り当てられたノード鍵に一方向性関数を施して、当該ノードのノード鍵を生成し、（ｂ）当該ノードの別の子ノードに割り当てられたノード鍵を用いて、生成した当該ノードのノード鍵を暗号化して暗号化ノード鍵を生成し、（ｃ）生成した暗号化ノード鍵を含む前記公開簿を生成し、

前記デバイス鍵特定手段は、前記木構造の１個のノードに対応するノード鍵を用いて公開された公開簿内の暗号化ノード鍵を復号した復号文、又は当該ノードに対応するノード鍵に一方向性関数を施して得られた出力値を選択し、選択した値を当該ノードの親ノードのノード鍵として求めることを特徴とする請求項２４に記載の利用者機器。

【請求項２７】　ｋを２以上の整数とし、ｍを０以上の整数とし、前記木構造をｋ分木とし、各ノード鍵を（ｘ，ｙ）平面上の点とみなし、

前記コンテンツ供給装置は、（ｘ，ｙ）平面上において、共通の親ノードを持つｋ個の全てのノードのノード鍵を結ぶ（ｋ＋ｍ－１）次の曲線を生成し、前記曲線上のノード鍵以外の（ｋ＋ｍ－１）個の点を含む前記公開簿を生成し、

前記デバイス鍵特定手段は、前記木構造の１個のノードに対応するノード鍵と、公開された公開簿内の（ｋ＋ｍ－１）個の点とを結ぶ、（ｋ＋ｍ－１）次の曲線を求め、さらにこの曲線から一方向性関数を用いて当該ノードの親ノードに対応するノード鍵を求めることを特徴とする請求項２４に記載の利用者機器。

【請求項２８】　前記コンテンツ供給装置は、（ａ）公開鍵暗号の秘密鍵と公開鍵のペアを生成し、（ｂ）生成した前記秘密鍵を秘密に保持し、生成した前記公開鍵を含む前記公開簿を生成し、（ｃ）前記木構造のリーフを除くノードについて、当該ノードに対応するノード鍵に基づいて、前記秘密鍵を用いて暗号化して暗号化ノード鍵を生成し、生成した暗号化ノード鍵を、当該ノードの子ノードに対応するノード鍵とし、（ｄ）前記公開簿を公開し、

前記デバイス鍵特定手段は、前記木構造の１個のノードに対応するノード鍵を、公開された公開簿内の公開鍵を用いて復号し、その結果を当該ノードの親ノードに対応するノード鍵とすることを特徴とする請求項２４に記載の利用者機器。

【請求項２９】　前記コンテンツ供給装置は、（ａ）秘密の素数ｐとｑの積ｎを計算し、（ｂ）ｐ－１とｑ－１の最小公倍数Ｌを求め、（ｃ）ｎと互いに素となるＬ以下の任意の整数ｅを求め、（ｄ）Ｌを法とするｅの逆元ｄを求めてこれを秘密鍵とし、（ｅ）前記整数ｅ及び前記積ｎを含む前記公開簿を生成し、（ｆ）前記ノードに対応するノード鍵と、当該ノードからその子ノードに接続する各パスに予め定められている個別のパス情報との排他的論理和を求め、（ｇ）排他的論理和を、前記秘密鍵ｄを用いて暗号化して暗号化ノード鍵を生成し、

（ｈ）生成した暗号化ノード鍵を当該パスに接続する子ノードに対応するノード鍵し、

前記デバイス鍵特定手段は、前記木構造の１個のノードに対応するノード鍵を、公開された公開簿内の公開鍵（ｅ、ｎ）を用いて復号し、その結果と、当該ノードの親ノードに接続するパスのパス情報との排他的論理和を求め、得られた排他的論理和を、当該ノードの親ノードに対応したノード鍵とすることを特徴とする請求項２８に記載の利用者機器。

【請求項３０】　前記コンテンツ供給装置は、

（Ａ）木構造のリーフとそのすぐ上位のノードの間に関しては、

（ａ）前記木構造のリーフのすぐ上位の各ノードについて、当該ノードに割り当てられたノード鍵を、当該ノードの子ノードに割り当てられたノード鍵を用いて暗号化して暗号化ノード鍵を生成し、生成した暗号化ノード鍵を含む前記公開簿を生成し、又は（ｂ）木構造のリーフのすぐ上位の各ノードについて、当該ノードの１個の子ノードに割り当てられたノード鍵に一方向性関数を施して、当該ノードのノード鍵を生成し、当該ノードの別の子ノードに割り当てられたノード鍵を用いて、生成した当該ノードのノード鍵を暗号化して暗号化ノード鍵を生成し、生成した暗号化ノード鍵を含む前記公開簿を生成し、又は（ｃ）ｋを２以上の整数とし、ｍを０以上の整

数とし、前記木構造をｋ分木とし、各ノード鍵を（ｘ，ｙ）平面上の点とみなし、（ｘ，ｙ）平面上において、共通の親ノードを持つｋ個の全てのリーフのノード鍵を結ぶ（ｋ＋ｍ－１）次の曲線を生成し、前記曲線上のノード鍵以外の（ｋ＋ｍ－１）個の点を含む前記公開簿を生成し、

（Ｂ）上記以外のノードの間に関しては、公開鍵暗号の秘密鍵と公開鍵のペアを生成し、生成した前記秘密鍵を秘密に保持し、生成した前記公開鍵を含む前記公開簿を生成し、前記木構造のリーフ及びすぐ上位のノードを除くノードについて、当該ノードに対応する ノード鍵に基づいて、前記秘密鍵を用いて暗号化して暗号化ノード鍵を生成し、生成した暗号化ノード鍵を、当該ノードの子ノードに対応するノード鍵とし、前記デバイス鍵特定手段は、

（Ａ）木構造のリーフとそのすぐ上位のノードの間に関しては、

（ａ）前記木構造の１個のリーフに対応するノード鍵を用いて、公開された公開簿内の暗号化ノード鍵を復号して、当該リーフの親ノードのノード鍵を求め、

（ｂ）前記木構造の１個のリーフに対応するノード鍵を用いて公開された公開簿内の暗号化ノード鍵を復号した復号文、又は当該リーフに対応するノード鍵に一方向性関数を施して得られた出力値を選択し、選択した値を当該リーフの親ノードのノード鍵として求め、又は（ｃ）前記木構造の１個のリーフに対応するノード鍵と、公開された公開簿内の（ｋ＋ｍ－１）個の点とを結ぶ、（ｋ＋ｍ－１）次の曲線を求め、さらにこの曲線から一方向性関数を用いて当該リーフの親ノードに対応するノード鍵を求め、

（Ｂ）上記以外のノードの間に関しては、前記木構造のリーフ及びすぐ上位のノードを除くノードに対応するノード鍵を、公開された公開簿内の公開鍵を用いて復号し、その結果を当該ノードの親ノードに対応するノード鍵とすることを特徴とする請求項２４に記載の利用者機器。

【請求項３１】　鍵管理装置と複数のシステム管理装置とが記同数のコンテンツ送出装置と１個の利用者機器とから構成されるデータ配信システムであって、各システム管理装置は、各コンテンツ送出装置に対応しており、各コンテンツ送出装置は、それぞれ暗号化コンテンツを供給し、前記利用者機器は、暗号化コンテンツを復号して利用し、

前記利用者機器へ当該利用者機器に固有の機器鍵を出力し、各システム管理装置について、前記機器鍵及び当該システム管理装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第１システム用機器鍵を生成し、生成した前記第１システム用機器鍵を当該システム管理装置へ出力する鍵管理装置と、

それぞれ、前記第１システム用機器鍵を受け取り、前記第１システム用機器鍵に基づいて、コンテンツを暗号化する際に基づくデバイス鍵を決定し、決定した前記デバイス鍵を対応する前記コンテンツ送出装置へ出力し、前記第１システム用機器鍵に基づいて、前記デバイス鍵を特定するための公開簿を生成し、生成した前記公開簿を公開する複数のシステム管理装置と、

それぞれ、前記デバイス鍵を受け取り、受け取った前記デバイス鍵に基づいて、デジタル著作物であるコンテンツを暗号化して暗号化コンテンツを生成し、前記暗号化コンテンツを前記利用者機器へ出力する複数のコンテンツ送出装置と、

前記機器鍵を受け取り、前記暗号化コンテンツを受け取り、公開された前記公開簿を取得し、前記機器鍵及び前記システム管理装置に固有のシステム情報に基づいて前記一方向性関数を用いて前記利用者機器に固有の第２システム用機器鍵を生成し、前記第２システム用機器鍵に基づいて、前記公開簿から前記デバイス鍵を特定し、特定した前記デバイス鍵に基づいて、受け取った前記暗号化コンテンツを復号して復号コンテンツを生成する１個の利用者機器とから構成されることを特徴とするデータ配信システム。

【請求項３２】　鍵管理装置で用いられる鍵管理方法であって、鍵管理装置と複数のコンテンツ供給装置と１個の利用者機器とから構成されるデータ配信システムにおける前記鍵管理装置は、前記利用者機器へ前記利用者機器に固有の機器鍵を供給し、各コンテンツ供給装置は、それぞれ暗号化コンテンツを供給し、前記利用者機器は、暗号化コンテンツを復号して利用し、

前記利用者機器へ当該利用者機器に固有の機器鍵を出力する機器鍵生成ステップと、

各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第１システム用機器鍵を生成し、生成した第１システム用機器鍵を前記コンテンツ供給装置へ出力するシステム用機器鍵生成ステップとを含むことを特徴とする鍵管理方法。

【請求項３３】　鍵管理装置で用いられる鍵管理用のコンピュータプログラムであって、鍵管理装置と複数のコンテンツ供給装置と１個の利用者機器とから構成されるデータ配信システムにおける前記鍵管理装置は、前記利用者機器へ前記利用者機器に固有の機器鍵を供給し、各コンテンツ供給装置は、それぞれ暗号化コンテンツを供給し、前記利用者機器は、暗号化コンテンツを復号して利用し、

前記利用者機器へ当該利用者機器に固有の機器鍵を出力する機器鍵生成ステップと、

各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第１システム用機器鍵を生成し、生成した第１システム用機器鍵を前

記コンテンツ供給装置へ出力するシステム用機器鍵生成ステップとを含むことを特徴とするコンピュータプログラム。

【請求項３４】　鍵管理装置で用いられる鍵管理用のコンピュータプログラムを記録しているコンピュータ読み取り可能な記録媒体であって、鍵管理装置と複数のコンテンツ供給装置と１個の利用者機器とから構成されるデータ配信システムにおける前記鍵管理装置は、前記利用者機器へ前記利用者機器に固有の機器鍵を供給し、各コンテンツ供給装置は、それぞれ暗号化コンテンツを供給し、前記利用者機器は、暗号化コンテンツを復号して利用し、

前記コンピュータプログラムは、

前記利用者機器へ当該利用者機器に固有の機器鍵を出力する機器鍵生成ステップと、

各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第１システム用機器鍵を生成し、生成した第１システム用機器鍵を前記コンテンツ供給装置へ出力するシステム用機器鍵生成ステップとを含むことを特徴とする記録媒体。

【請求項３５】　鍵管理装置と複数のコンテンツ供給装置と１個の利用者機器とから構成されるデータ配信システムにおける前記コンテンツ供給装置で用いられるコンテンツ供給方法であって、前記鍵管理装置は、前記利用者機器へ当該利用者機器に固有の機器鍵を出力し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第１システム用機器鍵を生成し、生成した前記第１システム用機器鍵を当該コンテンツ供給装置へ出力し、各コンテンツ供給装置は、前記鍵管理装置から前記第１システム用機器鍵を取得する取得ステップと、

前記第１システム用機器鍵に基づいて、デジタル著作物であるコンテンツを暗号化して暗号化コンテンツを生成する暗号ステップと、

生成した前記暗号化コンテンツを利用者機器へ出力する出力ステップとを含むことを特徴とするコンテンツ供給方法。

【請求項３６】　鍵管理装置と複数のコンテンツ供給装置と１個の利用者機器とから構成されるデータ配信システムにおける前記コンテンツ供給装置で用いられるコンテンツ供給用のコンピュータプログラムであって、前記鍵管理装置は、前記利用者機器へ当該利用者機器に固有の機器鍵を出力し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第１システム用機器鍵を生成し、生成した前記第

１システム用機器鍵を当該コンテンツ供給装置へ出力し、各コンテンツ供給装置は、デジタル著作物であるコンテンツを記憶している記憶手段を含み、

前記鍵管理装置から前記第１システム用機器鍵を取得する取得ステップと、

前記第１システム用機器鍵に基づいて、デジタル著作物であるコンテンツを暗号化して暗号化コンテンツを生成する暗号ステップと、

生成した前記暗号化コンテンツを利用者機器へ出力する出力ステップとを含むことを特徴とするコンピュータプログラム。

【請求項３７】　鍵管理装置と複数のコンテンツ供給装置と１個の利用者機器とから構成されるデータ配信システムにおける前記コンテンツ供給装置で用いられるコンテンツ供給用のコンピュータプログラムを記録している記録媒体であって、前記鍵管理装置は、前記利用者機器へ当該利用者機器に固有の機器鍵を出力し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第１システム用機器鍵を生成し、生成した前記第１システム用機器鍵を当該コンテンツ供給装置へ出力し、各コンテンツ供給装置は、デジタル著作物であるコンテンツを記憶している記憶手段を含み、

前記コンピュータプログラムは、

前記鍵管理装置から前記第１システム用機器鍵を取得する取得ステップと、

前記第１システム用機器鍵に基づいて、デジタル著作物であるコンテンツを暗号化して暗号化コンテンツを生成する暗号ステップと、

生成した前記暗号化コンテンツを利用者機器へ出力する出力ステップとを含むことを特徴とする記録媒体。

【請求項３８】　鍵管理装置と複数のコンテンツ供給装置と１個の利用者機器とから構成されるデータ配信システムにおける前記利用者機器で用いられる方法であって、前記鍵管理装置は、前記利用者機器へ当該利用者機器に固有の機器鍵を出力し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第１システム用機器鍵を生成し、生成した前記第１システム用機器鍵を当該コンテンツ供給装置へ出力し、各コンテンツ供給装置は、前記第１システム用機器鍵を受け取り、受け取った前記第１システム用機器鍵に基づいて、デジタル著作物であるコンテンツを暗号化して暗号化コンテンツを生成し、生成した前記暗号化コンテンツを利用者機器へ出力し、

前記鍵管理装置から前記機器鍵を受け取る取得ステップと、

前記コンテンツ供給装置から前記暗号化コンテンツを受け取る受信ステップと、

前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて前記一方向性関数を用いて前記利用者機器に固有の第２システム用機器鍵を生成するシステム用機器鍵生成ステップと、
生成した第２システム用機器鍵に基づいて、受け取った前記暗号化コンテンツを復号して復号コンテンツを生成する復号ステップとを含むことを特徴とする方法。
【請求項３９】　鍵管理装置と複数のコンテンツ供給装置と１個の利用者機器とから構成されるデータ配信システムにおける前記利用者機器で用いられるコンピュータプログラムであって、前記鍵管理装置は、前記利用者機器へ当該利用者機器に固有の機器鍵を出力し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第１システム用機器鍵を生成し、生成した前記第１システム用機器鍵を当該コンテンツ供給装置へ出力し、各コンテンツ供給装置は、前記第１システム用機器鍵を受け取り、受け取った前記第１システム用機器鍵に基づいて、デジタル著作物であるコンテンツを暗号化して暗号化コンテンツを生成し、生成した前記暗号化コンテンツを利用者機器へ出力し、前記鍵管理装置から前記機器鍵を受け取る取得ステップと、
前記コンテンツ供給装置から前記暗号化コンテンツを受け取る受信ステップと、
前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて前記一方向性関数を用いて前記利用者機器に固有の第２システム用機器鍵を生成するシステム用機器鍵生成ステップと、
生成した第２システム用機器鍵に基づいて、受け取った前記暗号化コンテンツを復号して復号コンテンツを生成する復号ステップとを含むことを特徴とするコンピュータプログラム。
【請求項４０】　鍵管理装置と複数のコンテンツ供給装置と１個の利用者機器とから構成されるデータ配信システムにおける前記利用者機器で用いられるコンピュータプログラムを記録しているコンピュータ読み取り可能な記録媒体であって、前記鍵管理装置は、前記利用者機器へ当該利用者機器に固有の機器鍵を出力し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第１システム用機器鍵を生成し、生成した前記第１システム用機器鍵を当該コンテンツ供給装置へ出力し、各コンテンツ供給装置は、前記第１システム用機器鍵を受け取り、受け取った前記第１システム用機器鍵に基づいて、デジタル著作物であるコンテンツを暗号化して暗号化コンテンツを生成し、生成した前記暗号化コンテンツを利用者機器へ出力し、
前記コンピュータプログラムは、
前記鍵管理装置から前記機器鍵を受け取る取得ステップと、
前記コンテンツ供給装置から前記暗号化コンテンツを受け取る受信ステップと、
前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて前記一方向性関数を用いて前記利用者機器に固有の第２システム用機器鍵を生成するシステム用機器鍵生成ステップと、
生成した第２システム用機器鍵に基づいて、受け取った前記暗号化コンテンツを復号して復号コンテンツを生成する復号ステップとを含むことを特徴とする記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、データを暗号化して配信する技術に関する。
【０００２】
【従来の技術】近年、映画や音楽などのデジタルコンテンツを、ＤＶＤ（Digital VersatileDisk）などのパッケージメディアや放送、通信を用いて、特定の機器に配信するビジネスが広がっている。このようなビジネスにおいて、コンテンツの著作権を保護するために、コンテンツは、暗号化されて特定の機器に配信される。特定の機器は、著作権者との合意による制限の下でのみ、予め機器に埋め込まれている機器鍵を用いて暗号化コンテンツを復号し、コンテンツの再生や複製を行う。
【０００３】大容量のコンテンツを配信する場合には、１個のグループ鍵を用いてコンテンツが暗号化され、さらにグループ鍵が特定の機器だけに共有できるよう暗号化されるという２段階の暗号方法を採るのが一般的である。本明細書では、このように個別の機器鍵を用いて１個のグループ鍵を共有する方法を、グループ鍵管理方法と呼ぶことにする。
【０００４】最も自明なグループ鍵管理方法では、コンテンツ供給者は、グループ鍵を各機器が備える機器鍵を用いて暗号化して暗号化鍵情報を生成し、この暗号化鍵情報を暗号化コンテンツと対応させて配信する。指定された機器は、暗号化鍵情報より自身の機器鍵を用いてグループ鍵を算出し、このグループ鍵を用いて暗号化コンテンツを復号する。しかしながら、自明な方法ではグループの構成メンバーが多い場合、暗号化鍵情報のデータ量が多くなる。そこで、如何にこのデータ量を削減して効率的にグループ鍵を配送するかに関して、多くの研究がなされている。
【０００５】中でも、各機器が複数の機器鍵を保持し、その共有関係を木構造で表現する木構造鍵管理方法は、インターネット上の新技術の標準化を検討しているＩＥＴＦ（The Internet Engineering Task Force）において盛んに議論されており、多くの研究成果が発表されている。木構造鍵管理方法において、基本的には木構造の各節はノードと呼ばれ、最下位のノードであるリーフに個々の機器が割り当てられる。各機器は、リーフから、

15

最上位のノードであるルートまでの経路上に存在するノードに対応するノード鍵を保管する。なお、ノードとノードを結ぶ経路をパスと呼ぶ。鍵管理者は、複数の機器が共通に保持するノード鍵を用いてグループ鍵を暗号化することにより、暗号化鍵情報を削減する。

【０００６】このような鍵管理方法が盛んに研究されている理由として、鍵管理者が新しい機器をグループに追加する場合や、何らかの理由で特定の機器をグループから排除する場合にも、情報量が少ない暗号化鍵情報によりグループ鍵を配布できること、あるノードをルートとした部分木を、現実の組織に対応させることにより、組織単位での追加や排除も可能であることなどが挙げられる。

【０００７】木構造を用いたグループ鍵管理方法を、代表的な木構造分割方法を例にして説明する。詳細は、非特許文献１に詳しく述べられている。

【非特許文献１】「デジタルコンテンツ保護用鍵管理方式（Key management system for digital content protection）」（中野稔久、大森基司、館林誠著、2001年暗号と情報セキュリティシンポジウム講演論文集、A5-5、2001－－－SCIS 2001,The 2001 Symposium on Cryptography and Information SecurityOiso,Japan,January 23-26,2001.The Institute of Electronics,Information and Communication Engineers）

【０００８】非特許文献１により開示されている木構造分割方法では、各機器は、それぞれ木のリーフに配置され、リーフからルートに至るすべてのノードに対応したノード鍵を保持する。図５４に示すように、機器１は、機器固有の鍵ｋｄ１及びＫｅｙＤ、ＫｅｙＢ、ＫｅｙＡを保持している。ＫｅｙＤは、機器１、２の共有鍵であり、ＫｅｙＢは、機器１～４の共有鍵であり、ＫｅｙＡは全機器共有の鍵である。

【０００９】システム管理者は、システムの運用を開始する時には、ルートの鍵であるＫｅｙＡでグループ鍵を暗号化して暗号化鍵情報を生成する。その後何らかの理由で、ある機器をグループからはずす必要が生じた時には、木構造からその機器が保持する鍵を取り除き、分割された複数の小さな木構造のルートの鍵でグループ鍵を暗号化して暗号化鍵情報を生成する。

【００１０】例えば、機器１をグループから排除された場合には、グループ鍵は、ＫｅｙＣ、ＫｅｙＥ、ｋｄ２を用いてそれぞれ暗号化される。ここでの各暗号文を、暗号化鍵情報と呼ぶことにする。グループ鍵を用いて暗号化されたコンテンツとともに、暗号化鍵情報は、コンテンツ供給者から配布される。これを受け取った機器（排除された機器を除く）は、自分が保持する機器鍵に対応した暗号化鍵情報よりグループ鍵を求め、コンテンツを復号する。

【００１１】また、非特許文献２は、予め機器が保有している機器鍵の増加を抑えながら、記録媒体に記録される鍵情報のサイズを小さくできる木構造パターン分割方式を開示している。

16

【００１２】

【非特許文献２】「デジタルコンテンツ保護用鍵管理方式 "木構造パターン分割方式"）（Key management system for digital content protection method"）」（中野稔久、大森基司、松崎なつめ、館林誠著）－－－SCIS 2002,The 2002 Symposium on Cryptography and InformationSecurity Shirahama,Japan,Jan.29-Feb.1,2002.The Institute ofElectronics,Information and Communication Engineers

【００１３】

【発明が解決しようとする課題】ところで、現在、運営主体、配信するコンテンツの種類、パッケージメディア、放送、インターネットなどの配信経路や媒体、提供されるサービスなどが異なる様々な複数のコンテンツ配信システムが、それぞれ独自の鍵管理方式を用いて、運営されているという問題がある。

【００１４】本発明は、１個の利用者機器が複数のコンテンツ供給システムに接続される場合に、それぞれのコンテンツ供給システムが柔軟で独自の鍵管理を行うことができるデータ配信システム、鍵管理装置、暗号化装置、利用者機器、これらを実現する方法、コンピュータプログラム及びコンピュータプログラムを記録している記録媒体を提供することを目的とする。

【００１５】

【課題を解決するための手段】本発明は、データを暗号化する複数の暗号化装置と、対応する暗号化装置用機器鍵を用いて暗号化データを復号する複数の機器からなるデータ配信システムであって、前記暗号化装置は、データを暗号化して機器に送付すると共に、前記暗号化装置用機器鍵を管理し、さらに公開簿を生成して機器に公開し、前記機器は、前記暗号化装置に対応した、暗号化装置用機器鍵と公開簿を用いて、前記暗号化データを復号することを特徴とする。

【００１６】ここで、前記データ配信システムは、前記公開簿が、前記暗号化装置に対応したＷｅｂページ、又はパッケージメディアを介して、機器に供給されるように構成してもよい。ここで、前記データ配信システムは、前記公開簿のうち、当該機器に対応したデータだけを切り出して機器に供給されるように構成してもよい。

【００１７】ここで、前記データ配信システムは、さらに、鍵管理機関を備え、前記鍵管理機関は、各暗号化装置に対応した各機器の暗号化装置用機器鍵を生成し、各機器と各暗号化装置に、対応した暗号化装置用機器鍵を供給するように構成してもよい。ここで、前記データ配信システムにおける前記鍵管理機関は、各機器の機器鍵を生成して機器に供給し、機器側にて前記機器鍵と暗号化装置に対応した識別情報を一方向性関数に入力し、その出力の暗号化装置用機器鍵を生成するように構成して

もよい。

【００１８】また、本発明は、データを暗号化して機器に送付する暗号化装置であって、暗号化装置用機器鍵を管理し、さらに公開簿を生成して機器に公開することを特徴とする。ここで、前記暗号化装置は、木構造を構築し、その各ノードに１つ以上のノード鍵を割り当てて、さらに、木構造のリーフに、前記各機器の、暗号化装置用機器鍵を割り当てて、前記暗号化装置用機器鍵とノード鍵を用いて公開簿を生成するように構成してもよい。

【００１９】ここで、前記暗号化装置は、前記公開簿に、リーフに割り当てられた暗号化装置用機器鍵のみを用いて、当該リーフからルートに至るノードに対応したノード鍵を順次求めるための情報を載せるように構成してもよい。ここで、前記暗号化装置は、前記公開簿に、あるノードに対応したノード鍵を、そのすべての子ノードに対応したそれぞれのノード鍵で暗号化した暗号文（第１の情報と呼ぶ）を載せるように構成してもよい。

【００２０】ここで、前記暗号化装置は、当該ノードの子ノードのうちの１つに対応したノード鍵を予め決められた一方向性関数を用いて変換した結果を、当該ノードに対応したノード鍵とし、公開簿には、これをその他の子ノードに対応したノード鍵で暗号化した暗号文（第２の情報と呼ぶ）を載せるように構成してもよい。ここで、前記暗号化装置は、ｋを２以上の整数、ｍを０以上の整数とし、各ノード鍵を（ｘ，ｙ）平面上の点とする場合、共通の親ノードを持つｋ個の全てのノードのノード鍵を結ぶ（ｋ＋ｍ－１）次の曲線を生成し、前記曲線上のノード鍵以外の（ｋ＋ｍ－１）個の点（第３の情報と呼ぶ）を公開簿に載せるように構成してもよい。

【００２１】ここで、前記暗号化装置は、前記（ｋ＋ｍ－１）次の曲線から一方向性関数を用いて予め決められた手法により一意に定まる点を、共通の親ノードに対応したノード鍵とするように構成してもよい。ここで、前記暗号化装置は、公開鍵暗号の秘密鍵と公開鍵のペアを生成し、秘密鍵を保持して公開鍵を前記公開簿に載せておき、一方、前記木構造のあるノードに対応したノード鍵を、前記公開鍵暗号の秘密鍵で暗号化した結果をその子ノードに対応したノード鍵とするように構成してもよい。ここで、公開簿に載せる情報を第４の情報と呼ぶ。

【００２２】ここで、前記暗号化装置は、秘密の素数ｐとｑの積ｎを計算して、ｐ－１とｑ－１の最小公倍数Ｌを求めて、ｎと互いに素となるＬ以下の任意の整数ｅを求めて、Ｌを法とするｅの逆元ｄを求めてこれを秘密鍵とし、前記（ｅ、ｎ）を公開鍵として公開簿に公開し、さらに、あるノードに対応したノード鍵と、当該ノードからその子ノードに接続する各パスに予め定められている個別のパス番号の排他的論理和を、前記秘密鍵ｄを用いて暗号化し、その結果を当該パスに接続する子ノードに対応したノード鍵とするように構成してもよい。

【００２３】ここで、前記暗号化装置は、木構造のリーフとそのすぐ上位のノードの間に関しては、前記第１、第２、又は第３の情報を公開簿に載せ、それ以外のノードの間に関しては、前記第４の情報を公開簿に載せるように構成してもよい。また、本発明は、暗号化装置により生成された暗号化データを復号する機器であって、暗号化装置用機器鍵と、前記暗号化装置に対応した公開簿を用いて、前記暗号化データを復号することを特徴とする。

【００２４】ここで、前記機器は、個別の機器鍵を保持し、前記機器鍵と前記暗号化装置の識別情報を用いて、対応する暗号化装置用機器鍵を生成するように構成してもよい。ここで、前記機器は、前記暗号化装置が定めた木構造のリーフに割り当てられ、対応した暗号化装置用機器鍵を保持するように構成してもよい。

【００２５】ここで、前記機器は、前記暗号化装置に対応した公開簿を用いて、前記木構造における、あるリーフに割り当てられた暗号化装置用機器鍵から、当該のリーフからルートに至るノードに対応したノード鍵を順次求めるように構成してもよい。ここで、前記機器は、前記木構造の、あるノードのノード鍵を用いて、公開簿内の対応する暗号文を復号し、当該ノードの親ノードのノード鍵を求めるように構成してもよい。

【００２６】ここで、前記機器は、前記木構造の、あるノードのノード鍵を用いて、公開簿内の対応する暗号文を復号した復号文、又は当該ノードのノード鍵を一方向関数に入力しその出力値のいずれかを選択して、当該ノードの親ノードのノード鍵として求めるように構成してもよい。ここで、前記機器は、前記木構造の、あるノードのノード鍵と、公開簿内の対応する（ｋ＋ｍ－１）個の点を結ぶ、（ｋ＋ｍ－１）次の曲線を求め、さらにこの曲線から一方向性関数を用いて当該ノードの親ノードのノード鍵として求めるように構成してもよい。

【００２７】ここで、前記機器は、前記木構造の、あるノードのノード鍵を、公開簿内の対応する公開鍵を用いて復号し、その結果を当該ノードの親ノードのノード鍵とするように構成してもよい。ここで、前記暗号化装置が、秘密の素数ｐとｑの積ｎを計算して、ｐ－１とｑ－１の最小公倍数Ｌを求めて、ｎと互いに素となるＬ以下の任意の整数ｅを求めて、Ｌを法とするｅの逆元ｄを求めて秘密鍵とし、前記（ｅ、ｎ）を公開鍵として公開簿に公開するとき、前記機器は、前記木構造のあるノードのノード鍵を、前記公開鍵（ｅ、ｎ）を用いて復号し、その結果と、当該ノードの親ノードに接続するパスのパス番号の排他的論理和を求めた結果を、当該ノードの親ノードに対応したノード鍵とするように構成してもよい。

【００２８】ここで、前記機器は、前記暗号化装置が、前記第１、第２又は第３の情報を載せた公開簿を用いて、木構造のリーフからそのすぐ上位のノードのノード鍵を求め、第４の情報を載せた公開簿を用いて、さらに

上位のノードのノード鍵を順次求めるように構成してもよい。

【００２９】

【発明の実施の形態】１．暗号化データ配信システム１

本発明に係る１個の実施の形態としての暗号化データ配信システム１について説明する。

１．１　暗号化データ配信システム１の構成

暗号化データ配信システム１は、図１に示すように、鍵管理装置１００、音楽配信システム管理装置２００、音楽コンテンツ配信装置３００、公開簿サーバ装置４００、ＤＶＤ供給システム管理装置５００、ＤＶＤ供給装置６００、公開簿供給装置７００、映画放送システム管理装置８００、映画コンテンツ供給装置９００、送信装置１０００、送信用アンテナ１０、放送衛星６、受信用アンテナ９、利用者機器１１００、図示していない他の複数の利用者機器及び製造装置１２００から構成されている。

【００３０】鍵管理装置１００は、製造装置１２００を介して、利用者機器１１００に固有の機器鍵ｋｄｉを利用者機器１１００へ配布する。また、鍵管理装置１００は、機器鍵ｋｄｉに基づいて生成したシステム用機器鍵$Skdi^{(i)}$、$Skdi^{(0)}$及び$Skdi^{(3)}$をそれぞれ、音楽配信システム管理装置２００、ＤＶＤ供給システム管理装置５００及び映画放送システム管理装置８００へ配布する。

【００３１】音楽配信システム２は、インターネット５を介して音楽のコンテンツを利用者に配信するコンテンツ供給システムであって、音楽配信システム管理装置２００、音楽コンテンツ配信装置３００、公開簿サーバ装置４００、利用者機器１１００及び他の利用者機器を含んで構成されている。音楽配信システム管理装置２００は、音楽配信システム２において用いられる暗号化のための鍵を管理し、後述する音楽用公開簿を公開簿サーバ装置４００を介して、利用者機器１１００等に公開する。音楽コンテンツ配信装置３００は、音楽配信システム管理装置２００により管理されている鍵に基づいて、音楽のコンテンツを暗号化して利用者機器１１００等へ送信する。利用者機器１１００等は、自身が記憶している機器鍵ｋｄｉ及び音楽用公開簿に基づいて、暗号化音楽コンテンツを復号して、音楽コンテンツを再生する。

【００３２】また、ＤＶＤ供給システム３は、映画などのコンテンツが記録されているＤＶＤを利用者に供給するコンテンツ供給システムであって、ＤＶＤ供給システム管理装置５００、ＤＶＤ供給装置６００、公開簿供給装置７００、利用者機器１１００及び他の利用者機器を含んで構成されている。ＤＶＤ供給システム管理装置５００は、ＤＶＤ供給システム３において用いられる暗号化のための鍵を管理し、後述するＤＶＤ用公開簿を、公開簿供給装置７００を介して、利用者機器１１００等に公開する。ＤＶＤ供給装置６００は、ＤＶＤ供給システム管理装置５００により管理されている鍵に基づいて、映画のコンテンツを暗号化してＤＶＤに記録し、暗号化映画コンテンツが記録されたＤＶＤは、利用者に供給される。利用者機器１１００等は、自身が記憶している機器鍵ｋｄｉ及びＤＶＤ用公開簿に基づいて、ＤＶＤに記録されている暗号化映画コンテンツを復号して、映画コンテンツを再生する。

【００３３】さらに、映画放送システム４は、映画などのコンテンツを放送波に載せて利用者に供給するコンテンツ供給システムであって、映画放送システム管理装置８００、映画コンテンツ供給装置９００、送信装置１０００、送信用アンテナ１０、放送衛星６、受信用アンテナ９、利用者機器１１００及び他の利用者機器を含んで構成されている。映画放送システム管理装置８００は、映画放送システム４において用いられる暗号化のための鍵を管理し、送信装置１０００及び放送衛星６を介して、後述する映画用公開簿を放送波により放送することにより、利用者機器１１００等に公開する。映画コンテンツ供給装置９００は、映画放送システム管理装置８００により管理されている鍵に基づいて、映画のコンテンツを暗号化し、送信装置１０００及び放送衛星６を介して、暗号化映画コンテンツを放送波により放送することにより、利用者に供給する。利用者機器１１００等は、放送波を受信し、受信した放送波から暗号化映画コンテンツを抽出し、自身が記憶している機器鍵ｋｄｉ及び映画用公開簿に基づいて、抽出した暗号化映画コンテンツを復号して、映画コンテンツを再生する。

【００３４】１．２　鍵管理装置１００の構成

鍵管理装置１００は、鍵管理機関が有しており、鍵管理機関により管理及び運営がさなされている。鍵管理機関は、各利用者機器の機器鍵を生成して管理する信頼のおける機関である。鍵管理装置１００は、利用者機器１１００に固有の機器鍵ｋｄｉを生成し、生成した機器鍵ｋｄｉを、製造装置１２００を介して、利用者機器１１００へ配布する。ここで、鍵管理装置１００により生成された機器鍵ｋｄｉが、可搬型の記録媒体に書き込まれ、鍵管理装置１００を有する鍵管理機関は、前記記録媒体を製造装置１２００を有する製造業者に手渡す。なお、鍵管理装置１００と製造装置１２００とは、通信回線により接続されており、鍵管理装置１００は、前記通信回線を介して製造装置１２００へ、機器鍵ｋｄｉを安全な通信プロトコルを用いて、送信するとしてもよい。

【００３５】また、鍵管理装置１００は、それぞれ、音楽配信システム管理装置２００、ＤＶＤ供給システム管理装置５００及び映画放送システム管理装置８００と通信回線により接続されている。鍵管理装置１００は、機器鍵ｋｄｉに基づいて、それぞれ、音楽配信システム管理装置２００、ＤＶＤ供給システム管理装置５００及び映画放送システム管理装置８００で用いるためのシステム用機器鍵$Skdi^{(1)}$、$Skdi^{(2)}$及び$Skdi$

(3) を生成し、生成したシステム用機器鍵Ｓｋｄｉ(2)、Ｓｋｄｉ(2) 及びＳｋｄｉ(3) をそれぞれ、前記通信回線を介して、安全な通信プロトコルを用いて、音楽配信システム管理装置２００、ＤＶＤ供給システム管理装置５００及び映画放送システム管理装置８００へ送信する。

【００３６】鍵管理装置１００は、図２に示すように、入力部１０１、制御部１０２、表示部１０３、機器鍵生成部１０４、システム用機器鍵生成部１０５、機器鍵出力部１０６、情報記憶部１０７及びシステム用機器鍵送信部１０８から構成されている。鍵管理装置１００は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、ディスプレイユニット、キーボード、マウス、通信ユニットなどから構成されるコンピュータシステムである。前記ＲＡＭ又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、鍵管理装置１００は、その機能を達成する。

【００３７】（１）情報記憶部１０７

情報記憶部１０７は、機器鍵管理テーブル１１１及びシステム用機器鍵管理テーブル１２１を有する。

（機器鍵管理テーブル１１１）機器鍵管理テーブル１１１は、図３に示すように、機器ＩＤと機器鍵ｋｄｉとからなる機器情報を複数個記憶するための領域を備えている。

【００３８】機器ＩＤは、利用者機器を識別するための識別情報であり、具体的には、利用者機器の製造番号である。機器鍵ｋｄｉは、当該利用者機器に割り当てられる固有の鍵情報である。

（システム用機器鍵管理テーブル１２１）システム用機器鍵管理テーブル１２１は、図４に示すように、機器ＩＤとシステムＩＤとシステム用機器鍵Ｓｋｄｉ(0) とからなるシステム情報を複数個記憶するための領域を備えている。

【００３９】機器ＩＤは、上述したように、利用者機器を識別するための識別情報である。システムＩＤは、音楽配信システム２、ＤＶＤ供給システム３及び映画放送システム４に代表されるような、コンテンツを供給したり配信したりするコンテンツ供給システムを識別するための識別子である。ここでは、具体的には、音楽配信システム２、ＤＶＤ供給システム３及び映画放送システム４を識別するシステムＩＤは、それぞれ、「１」、「２」及び「３」である。

【００４０】システム用機器鍵Ｓｋｄｉ(0) は、各コンテンツ供給システムにおいて、利用者機器に割り当てられる固有の鍵情報である。Ｓｋｄｉ(0) において、サフィックスｉは、当該利用者機器の機器ＩＤに対応するものであり、サフィックスｊは、当該コンテンツ供給システムのシステムＩＤに対応するものである。

（２）制御部１０２

制御部１０２は、機器鍵及びシステム用機器鍵の生成が終了するまで、機器鍵及びシステム用機器鍵の生成の処理を繰り返すように、鍵管理装置１００の各構成部を制御する。

【００４１】また、制御部１０２は、鍵管理機関の運営者から入力部１０１を介して、システムＩＤ及び機器１Ｄの入力を受け付ける。制御部１０２は、機器１Ｄの入力を受け付けると、機器鍵管理テーブル１１１内に、入力を受け付けた前記機器ＩＤが記憶されているか否かを判断し、前記機器ＩＤが機器鍵管理テーブル１１１に記憶されていないと判断する場合に、機器ＩＤを機器鍵生成部１０４へ出力し、機器鍵生成部１０４に対して機器鍵を新たに生成するように指示する。

【００４２】一方、制御部１０２は、入力を受け付けた前記機器ＩＤが機器鍵管理テーブル１１１に記憶されていると判断する場合に、機器鍵管理テーブル１１１から前記機器ＩＤを含む機器情報を読み出し、読み出した機器情報から機器鍵ｋｄｉを抽出し、抽出した機器鍵ｋｄｉをシステム用機器鍵生成部１０５へ出力する。

（３）機器鍵生成部１０４

機器鍵生成部１０４は、制御部１０２から機器ＩＤ及び機器鍵を新たに生成する旨の指示を受け取る。

【００４３】前記指示を受け取ると、機器鍵生成部１０４は、乱数を生成し、生成した乱数を用いて、新たに機器鍵ｋｄｉを生成する。次に、機器鍵生成部１０４は、受け取った機器ＩＤと生成した機器鍵ｋｄｉとを機器鍵出力部１０６へ出力し、生成した機器鍵ｋｄｉをシステム用機器鍵生成部１０５へ出力し、受け取った前記機器ＩＤと生成した機器鍵ｋｄｉとから構成される機器情報を機器鍵管理テーブル１１１へ書き込む。

【００４４】（４）システム用機器鍵生成部１０５

システム用機器鍵生成部１０５は、機器鍵生成部１０４から機器鍵ｋｄｉを受け取り、制御部１０２からシステムＩＤを受け取り、受け取った機器鍵ｋｄｉとシステムＩＤとを結合して結合情報を得、得られた結合情報に一方向性関数ｈを施して、システム用機器鍵Ｓｋｄｉ(3) を生成する。

【００４５】システム用機器鍵Ｓｋｄｉ(0) ＝ｈ（ｋｄｉ、システムＩＤ）

ここで、ｈ（Ａ、Ｂ）は、ＡとＢとの結合情報に一方向性関数ｈを施すことを示す。また、一方向性関数ｈの一例は、ＳＨＡ－１である。次に、システム用機器鍵生成部１０５は、システムＩＤ及び生成したシステム用機器鍵Ｓｋｄｉ(3) をシステム用機器鍵送信部１０８へ出力する。

【００４６】また、システム用機器鍵生成部１０５は、機器ＩＤ、システムＩＤ及びシステム用機器鍵Ｓｋｄｉ(3) を対応付けて構成されるシステム情報をシステム用機器鍵管理テーブル１２１へ書き込む。

（５）機器鍵出力部１０６
機器鍵出力部１０６は、機器鍵生成部１０４から機器ＩＤ及び機器鍵ｋｄｉを受け取り、利用者機器に機器鍵が割り当てられていない場合に、機器ＩＤ及び機器鍵ｋｄｉを製造装置１２００を介して利用者機器へ出力する。
【００４７】（６）システム用機器鍵送信部１０８
システム用機器鍵送信部１０８は、通信回線を介して、音楽配信システム管理装置２００、ＤＶＤ供給システム管理装置５００及び映画放送システム管理装置８００と接続されている。システム用機器鍵送信部１０８は、システム用機器鍵生成部１０５からシステムＩＤ及びシステム用機器鍵$Skdi^{(t)}$を受け取り、制御部１０２から機器ＩＤを受け取る。次に、システム用機器鍵送信部１０８は、システムＩＤにより示されるシステム用管理装置へ、通信回線を介して、機器ＩＤとシステム用機器鍵$Skdi^{(t)}$を送信する。
【００４８】（７）入力部１０１
入力部１０１は、鍵管理機関の運営者から、システムＩＤ及び機器ＩＤの入力を受け付け、入力を受け付けたシステムＩＤ及び機器ＩＤを制御部１０２へ出力する。
（８）表示部１０３
表示部１０３は、各種情報を表示する。
【００４９】１．３　音楽配信システム管理装置２００の構成
音楽配信システム管理装置２００は、音楽配信システム２において用いられる暗号化のための鍵を管理し、暗号化のためのノード鍵を音楽コンテンツ配信装置３００へ出力し、また後述する音楽用公開簿をサーバ装置４００を介して、利用者機器１１００等に公開する。
【００５０】音楽配信システム管理装置２００は、図５に示すように、表示部２０１、制御部２０２、入力部２０３、木構造構築部２０４、ノード鍵生成部２０５、公開簿生成部２０６、送受信部２０７及び情報記憶部２０８から構成されている。音楽配信システム管理装置２００は、鍵管理装置１００と同様のコンピュータシステムである。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、音楽配信システム管理装置２００は、その機能を達成する。
【００５１】（１）情報記憶部２０８
情報記憶部２０８は、音楽配信用木構造テーブル２１１及び音楽用公開簿２２１を有している。音楽配信用木構造テーブル２１１は、図６に一例として示す木構造Ｔ１００に対応しており、木構造Ｔ１００を表現するためのデータ構造を示している。
【００５２】後述するように、木構造構築部２０４により、木構造Ｔ１００を表現するためのデータ構造が音楽配信用木構造テーブル２１１として生成され、情報記憶部２０８に書き込まれる。
（木構造Ｔ１００）木構造Ｔ１００は、図６に示すように、階層１から階層４までの４階層からなる２分木である。木構造Ｔ１００は、２分木であるので、木構造Ｔ１００が有する各ノード（リーフを除く）は、２本のパスを介して下位側の２個のノードにそれぞれ接続されている。階層１にはルートである１個のノードが含まれ、階層２には２個のノードが含まれ、階層３には４個のノードが含まれ、階層４にはリーフである８個のノードが含まれている。なお、木構造において下位側とはリーフ側を示し、上位側とはルート側を示している。
【００５３】木構造Ｔ１００が有する各ノード（リーフを除く）と、下位側のノードとを接続する複数のパスについて、左側のパスから右側のパスへの順に、「１」、「２」、・・・などの番号が割り当てられている。ここで、図６の紙面において、各ノードを中心として当該ノードから左側下方に接続されているパスを左のパスと称し、当該ノードから右側下方に接続されているパスを右のパスと称している。
【００５４】各ノードには、ノード番号が付されている。階層１に属するルートであるノードのノード番号は、「１」である。また、階層２を含め、階層２より下位にある階層に属するノードに対しては、左側のノードから右側のノードへの順に、「１」、「２」、・・・などの番号が割り当てられている。ここで、左及び右とは、上述した通りである。例えば、階層２に属する２個のノードのノード番号は、それぞれ「１」及び「２」である。また、階層３に属する４個のノードのノード番号は、それぞれ「１」、「２」、「３」及び「４」である。
【００５５】また、木構造Ｔ１００が有する各ノードのうち、最下層に属するノード、即ちリーフには、それぞれ、リーフ番号が割り当てられている。具体的には、図６に示すように、階層４に属する８個のリーフ（ノード番号は、「１」、「２」、・・・、「８」）には、それぞれ、リーフ番号「０００」、「００１」、「０１０」、・・・、「１１１」が割り当てられている。ここで、リーフ番号は、２進数により表現されている。
【００５６】ここで、リーフ番号の定め方について説明する。木構造Ｔ１００が有する各ノード（リーフを除く）と、下位に接続されるノードとを接続する２本のパスのうち、その一方である左のパスには、「０」の番号を割り当て、他方である右のパスには「１」の番号を割り当てる。これらの番号は、２進数により表現される１ビットの値である。このような規則により、木構造Ｔ１００が有する全てのパスに、「０」又は「１」の番号を割り当てるとすると、ルートからあるリーフへたどる経路に含まれる複数のパスにそれぞれ割り当てられた番号を用いて、ルートから前記リーフへたどる前記経路を一意に識別することができる。このルートから前記リーフへたどる前記経路は、前記リーフに一対一に対応しているので、これらの番号は、前記リーフを識別するとも言える。

【００５７】リーフ番号は、ルートから当該リーフへたどる経路に含まれる複数のパスにそれぞれ割り当てられた番号を、この順序で並べることにより、構成される。例えば、リーフ番号「０００」は、ルートから左のパスをたどって、階層２のノードに至り、さらに左のパスをたどって、階層３のノードに至り、さらに左のパスをたどって至る階層４のリーフを示している。

【００５８】木構造Ｔ１００が有する各ノードには、ノード鍵が割り当てられる。具体的には、図６に示すように、階層１に属するルートには、ノード鍵「$KeyA^{(1)}$」が割り当てられる。また、階層２に属する２個のノード（ノード番号は、「１」及び「２」）には、それぞれ、ノード鍵「$KeyB^{(0)}$」及びノード鍵「$KeyC^{(1)}$」が割り当てられる。階層３及び階層４に属するノードについても同様である。

【００５９】また、木構造Ｔ１００が有する各リーフには、利用者機器が割り当てられる。具体的には、図６に示すように、各リーフに、利用者機器を識別する機器ＩＤが割り当てられる。

（音楽配信用木構造テーブル２１１）音楽配信用木構造テーブル２１１は、図７に示すように、木構造Ｔ１００に含まれるノードと同じ数のノード情報を含んで構成されており、各ノード情報は、木構造Ｔ１００を構成する各ノードにそれぞれ対応している。

【００６０】各ノード情報は、リーフを除くノードについては、階層番号、ノード番号及びノード鍵を含み、リーフについては、階層番号、ノード番号、ノード鍵及び機器ＩＤを含む。階層番号は、当該ノード情報に対応するノードが属する階層を示す番号である。

【００６１】ノード番号は、前記階層内において、当該ノード情報に対応するノードを識別するための番号である。ノード鍵は、当該ノード情報に対応するノードに対して割り当てられた鍵である。また、機器ＩＤは、リーフであるノードに対応するノード情報のみに含まれ、リーフ以外のノードに対応するノード情報には含まれない。機器ＩＤは、リーフに割り当てられる利用者機器を識別する識別情報である。

【００６２】（音楽用公開簿２２１）音楽用公開簿２２１は、図８に示すように、システムＩＤ及び所定数個の公開情報を含んで構成されている。各公開情報は、インデックス情報及び暗号化ノード鍵を含む。ここで、前記所定数は、木構造Ｔ１００に含まれるノード（リーフを除く）の個数の２倍の数であり、木構造Ｔ１００に含まれる各ノードは、音楽用公開簿２２１に含まれる２個の公開情報に対応している。

【００６３】システムＩＤは、上述したとおりであって、コンテンツを供給したり配信したりするコンテンツ供給システムを識別するための識別子である。インデックス情報は、階層番号及びパス番号を含む。ここで、階層番号は、当該公開情報に対応するノードが属する階層を示す番号である。また、パス番号は、当該公開情報に対応するノードから下位のノードへのパスを示す番号である。木構造Ｔ１００は、２分木であるので、各ノード（リーフを除く）から下位のノードへのパスは、２本存在する。

【００６４】暗号化ノード鍵は、対応するノードに割り当てられたノード鍵に、対応するパス番号により示されるパスにより接続される下位ノードに割り当てられたノード鍵を鍵として、暗号化アルゴリズムＥ１を施して生成されたものである。ここで、暗号化アルゴリズムＥ１は、一例として、ＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）によるものである。

【００６５】また、この明細書において、鍵Ａを用いて、平文Ｂに暗号化アルゴリズムＥ１を施して得られる暗号文をＥ１（Ａ、Ｂ）と表現する。音楽用公開簿２２１に含まれる公開情報の一例は、図８に示すように、（３、１）及び$E1(Skd1^{(0)}, KeyD^{(0)})$を含む。ここで、（３、１）は、階層番号が３であり、パス番号が１であることを示している。また、$E1(Skd1^{(0)}, KeyD^{(0)})$は、$Skd1^{(0)}$を鍵として用いて、$KeyD^{(0)}$に暗号化アルゴリズムＥ１を施して得られる暗号文であることを示している。

【００６６】（２）木構造構築部２０４

木構造構築部２０４は、音楽配信用木構造テーブル２１１を生成して情報記憶部２０８へ書き込む。具体的には、木構造構築部２０４は、木構造Ｔ１００に含まれる各ノードについて、階層番号とノード番号とを含むノード情報を生成し、生成したノード情報を音楽配信用木構造テーブル２１１内に書き込む。なお、この時点では、各ノード情報には、ノード鍵及び機器ＩＤは、含まれていない。

【００６７】木構造構築部２０４は、鍵管理装置１００から、制御部２０２を介して、機器ＩＤ及びシステム用機器鍵$Skd1^{(0)}$を受け取り、音楽配信用木構造テーブル２１１において、受け取ったシステム用機器鍵$Skd1^{(0)}$が１個のリーフに対応するように、受け取った機器ＩＤ及びシステム用機器鍵$Skd1^{(0)}$を音楽配信用木構造テーブル２１１に書き込む。また、前記リーフを示すリーフ番号を制御部２０２へ出力する。

【００６８】このように、木構造において、システム用機器鍵がリーフに割り当てられ、他のノードにノード鍵が割り当てられる。

（３）制御部２０２

制御部２０２は、機器ＩＤ及びシステム用機器鍵$Skd1^{(0)}$の受取りが終了するまで、機器ＩＤ及びシステム用機器鍵$Skd1^{(0)}$の受取りと、システム用機器鍵の音楽配信用木構造テーブル２１１への書込みと、利用者機器へのリーフ番号の送信とを繰り返すように制御する。

【００６９】制御部２０２は、鍵管理装置１００から送

受信部２０７を介して、機器ＩＤ及びシステム用機器鍵Ｓｋｄｉ$^{(0)}$を受け取り、受け取った機器ＩＤ及びシステム用機器鍵Ｓｋｄｉ$^{(0)}$を木構造構築部２０４へ出力する。また、制御部２０２は、木構造構築部２０４からリーフ番号を受け取り、送受信部２０７及びインターネット５を介して、受け取った機器ＩＤにより示される利用者機器へ、システムＩＤ（＝１）と受け取ったリーフ番号とを送信する。

【００７０】さらに、制御部２０２は、音楽配信用木構造テーブル２１１から、所定の基準に基づいて、１個のノード鍵を選択する。ここでは、一例として、リーフからルートへの経路上に存在する全てのノードのうち、最上位のノード即ちルートに割り当てられたノード鍵を選択する。なお、ここで選択したノード鍵をデバイス鍵と称することもある。次に、制御部２０２は、選択したノード鍵を、音楽コンテンツ配信装置３００へ送信する。前記デバイス鍵は、利用者機器がコンテンツを復号する際に基づく鍵である。このように、前記木構造を用いて管理されている１個以上のノード鍵の中から前記デバイス鍵が決定される。

【００７１】（４）ノード鍵生成部２０５

制御部２０２が、機器ＩＤ及びシステム用機器鍵Ｓｋｄｉ$^{(0)}$の受取りが終了したと判断する場合に、ノード鍵生成部２０５は、音楽配信用木構造テーブル２１１の各ノード（リーフを除く）について、乱数を生成し、生成した乱数を用いてノード鍵を生成し、生成したノード鍵を各ノードに対応付けて、音楽配信用木構造テーブル２１１へ書き込む。

【００７２】（５）公開簿生成部２０６

公開簿生成部２０６は、音楽用公開簿２２１を生成し、生成した音楽用公開簿２２１を情報記憶部２０８に書き込み、生成した音楽用公開簿２２１を、公開簿サーバ装置４００へ送信する。なお、公開簿生成部２０６による音楽用公開簿２２１の生成の詳細については、後述する。

【００７３】（６）送受信部２０７

送受信部２０７は、通信回線を介して、音楽コンテンツ配信装置３００と接続され、また、インターネット５を介して、利用者機器１１００と接続されている。送受信部２０７は、制御部２０２と音楽コンテンツ配信装置３００との間で情報の送受信を行う。また、送受信部２０７は、制御部２０２と利用者機器１１００との間で情報の送受信を行う。

【００７４】（７）表示部２０１及び入力部２０３

表示部２０１は、制御部２０２の制御の元に各種の情報を表示する。また、入力部２０３は、音楽配信システム管理装置２００の管理者からの情報の入力を受け付ける。

１．４　公開簿サーバ装置４００の構成

公開簿サーバ装置４００は、音楽配信システム管理装置２００と通信回線を介して接続されており、通信回線を介して、音楽配信システム管理装置２００から音楽用公開簿を受信し、受信した音楽用公開簿を内部に記憶する。また、公開簿サーバ装置４００は、インターネット５を介して、利用者機器１１００と接続されており、利用者機器１１００からの要求に応じて、内部に記憶している音楽用公開簿を、インターネット５を介して、利用者機器１１００へ送信する。

【００７５】公開簿サーバ装置４００は、図９に示すように、情報記憶部４０１、送受信部４０２、制御部４０３、入力部４０４及び表示部４０５から構成されている。公開簿サーバ装置４００は、鍵管理装置１００と同様のコンピュータシステムである。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、公開簿サーバ装置４００は、その機能を達成する。

【００７６】情報記憶部４０１は、情報を記憶するための領域を備える。送受信部４０２は、通信回線を介して、音楽配信システム管理装置２００と接続されている。また、送受信部４０２は、インターネット５を介して、利用者機器１１００と接続されている。制御部４０３は、音楽配信システム管理装置２００から、通信回線及び送受信部４０２を介して、音楽用公開簿を受信し、受信した音楽用公開簿を情報記憶部４０１へ書き込む。

【００７７】また、制御部４０３は、利用者機器１１００から、インターネット５を介して、音楽用公開簿の送信要求を受け取る。前記送信要求を受け取ると、制御部４０３は、情報記憶部４０１から音楽用公開簿を読み出し、読み出した音楽用公開簿を、インターネット５を介して、利用者機器１１００へ送信する。入力部４０４は、公開簿サーバ装置４００の管理者からの入力を受け付ける。

【００７８】表示部４０５は、制御部４０３の制御により各種の情報を表示する。

１．５　音楽コンテンツ配信装置３００の構成

音楽コンテンツ配信装置３００は、音楽配信システム管理装置２００から受け取ったノード鍵を用いてグループ鍵を暗号化し、グループ鍵を用いて音楽情報を暗号化し、暗号化グループ鍵及び暗号化音楽情報を、利用者機器１１００へ送信する。

【００７９】音楽コンテンツ配信装置３００は、図１０に示すように、情報記憶部３０１、グループ鍵生成部３０２、暗号化部３０３、ノード鍵取得部３０４、暗号化部３０５、送受信部３０６、制御部３０７、入力部３０８及び表示部３０９から構成されている。図１０において、各ブロックは、音楽コンテンツ配信装置３００の構成要素を示しており、接続線により他のブロックと接続されている。ここで、各接続線は、信号や情報が伝達される経路を示している。また、暗号化部３０５を示すブロックに接続している複数の接続線のうち、接続線上に鍵マークが付されているものは、暗号化部３０５へ鍵と

しての情報が伝達される経路を示している。暗号化部３０３を示すブロックについても同様である。また、他の図面についても同様である。

【００８０】音楽コンテンツ配信装置３００は、鍵管理装置１００と同様のコンピュータシステムである。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、音楽コンテンツ配信装置３００は、その機能を達成する。

（１）情報記憶部３０１

情報記憶部３０１は、予め、複数個の音楽情報を記憶している。

（２）ノード鍵取得部３０４

ノード鍵取得部３０４は、通信回線を介して、音楽配信システム管理装置２００に接続されており、音楽配信システム管理装置２００から、通信回線を介して、ノード鍵を受信し、受信したノード鍵を、ノード鍵Ｎｋとして暗号化部３０５へ出力する。

（３）グループ鍵生成部３０２

グループ鍵生成部３０２は、乱数を生成し、生成した乱数を用いて、グループ鍵Ｇを生成し、生成したグループ鍵Ｇを暗号化部３０５及び暗号化部３０３へ出力する。

（４）暗号化部３０５

暗号化部３０５は、ノード鍵取得部３０４からノード鍵Ｎｋを受け取り、グループ鍵生成部３０２からグループ鍵Ｇを受け取る。

【００８１】次に、暗号化部３０５は、受け取ったノード鍵Ｎｋを用いて、受け取ったグループ鍵Ｇに暗号化アルゴリズムＥ３を施して、暗号化グループ鍵Ｅ３（Ｎｋ、Ｇ）を生成する。ここで、暗号化アルゴリズムＥ３は、一例としてＤＥＳによるアルゴリズムである。

【００８２】次に、暗号化部３０５は、生成した暗号化グループ鍵Ｅ３（Ｎｋ、Ｇ）を送受信部３０６へ出力する。

（５）暗号化部３０３

暗号化部３０３は、情報記憶部３０１から音楽情報ＭＣを読み出し、また、グループ鍵生成部３０２からグループ鍵Ｇを受け取る。

【００８３】グループ鍵Ｇを受け取ると、暗号化部３０３は、受け取ったグループ鍵Ｇを鍵として用いて、読み出した音楽情報ＭＣに暗号化アルゴリズムＥ２を施して、暗号化音楽情報Ｅ２（Ｇ、ＭＣ）を生成する。ここで、暗号化アルゴリズムＥ２は、一例としてＤＥＳによるアルゴリズムである。

【００８４】次に、暗号化部３０３は、生成した暗号化音楽情報Ｅ２（Ｇ、ＭＣ）を送受信部３０６へ出力する。

（６）送受信部３０６

送受信部３０６は、暗号化部３０５から暗号化グループ鍵Ｅ３（Ｎｋ、Ｇ）を受け取り、暗号化部３０３から暗号化音楽情報Ｅ２（Ｇ、ＭＣ）を受け取る。

【００８５】次に、送受信部３０６は、利用者機器１１００から受け取った当該利用者の要求に応じて、暗号化グループ鍵Ｅ３（Ｎｋ、Ｇ）と暗号化音楽情報Ｅ２（Ｇ、ＭＣ）とを、インターネット５を介して、利用者機器１１００へ送信する。

（７）制御部３０７、入力部３０８及び表示部３０９

制御部３０７は、音楽コンテンツ配信装置３００の各構成要素を制御する。入力部３０８は、音楽コンテンツ配信装置３００の管理者からの入力を受け付ける。表示部３０９は、各種の情報を表示する。

【００８６】１．６　ＤＶＤ供給システム管理装置５００の構成

ＤＶＤ供給システム管理装置５００は、ＤＶＤ供給システム３において用いられる暗号化のための鍵を管理し、後述するＤＶＤ用公開簿を、公開簿供給装置７００を介して、利用者機器１１００等に公開する。ＤＶＤ供給システム管理装置５００は、図１１に示すように、表示部５０１、制御部５０２、入力部５０３、木構造構築部５０４、ノード鍵生成部５０５、公開簿生成部５０６、送受信部５０７及び情報記憶部５０８から構成されている。

【００８７】ＤＶＤ供給システム管理装置５００は、鍵管理装置１００と同様のコンピュータシステムである。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、ＤＶＤ供給システム管理装置５００は、その機能を達成する。

（１）情報記憶部５０８

情報記憶部５０８は、ＤＶＤ用木構造テーブル５１１及びＤＶＤ用公開簿５２１を有している。

【００８８】ＤＶＤ用木構造テーブル５１１は、図１３に一例として示す木構造Ｔ２００に対応しており、木構造Ｔ２００を表現するためのデータ構造を示している。後述するように、木構造構築部５０４により、木構造Ｔ２００を表現するためのデータ構造がＤＶＤ用木構造テーブル５１１として生成され、情報記憶部５０８に書き込まれる。

【００８９】（木構造Ｔ２００）木構造Ｔ２００は、図１３に示すように、階層１から階層４までの４階層からなる２分木である。木構造Ｔ２００は、木構造Ｔ１００と同様の構造を有しているので、詳細の説明は、省略する。

（ＤＶＤ用木構造テーブル５１１）ＤＶＤ用木構造テーブル５１１は、図１２に示すように、木構造Ｔ２００に含まれるノードと同じ数のノード情報を含んで構成されており、各ノード情報は、木構造Ｔ２００を構成する各ノードにそれぞれ対応している。ＤＶＤ用木構造テーブル５１１は、音楽配信用木構造テーブル２１１と同じデータ構造を有している。

【００９０】各ノード情報は、リーフを除くノードについては、階層番号、ノード番号及びノード鍵を含み、リ

ーフについては、階層番号、ノード番号、ノード鍵及び機器ＩＤを含む。なお、階層番号、ノード番号、ノード鍵及び機器ＩＤについては、上述しているので、説明を省略する。

（ＤＶＤ用公開簿５２１）ＤＶＤ用公開簿５２１は、図１４に示すように、システムＩＤ及び所定数個の公開情報を含んで構成されている。各公開情報は、インデックス情報及び暗号化ノード鍵を含む。

【００９１】ここで、前記所定数は、木構造Ｔ２００に含まれるノード（リーフを除く）の個数であり、木構造Ｔ２００に含まれる各ノード（リーフを除く）は、それぞれ、ＤＶＤ用公開簿５２１に含まれる公開情報に対応している。システムＩＤは、上述したとおりであって、コンテンツを供給したり配信したりするコンテンツ供給システムを識別するための識別子である。

【００９２】インデックス情報は、階層番号及びノード番号を含む。ここで、階層番号は、当該公開情報に対応するノードが属する階層を示す番号である。また、ノード番号は、当該公開情報に対応するノードを示す番号である。暗号化ノード鍵は、対応するノードに割り当てられたノード鍵に、当該ノードの右下側に接続する下位ノードに割り当てられたノード鍵を鍵として用いて、暗号化アルゴリズムＥ４を施して生成されたものである。

【００９３】ここで、暗号化アルゴリズムＥ４は、一例として、ＤＥＳによるものである。ＤＶＤ用公開簿５２１に含まれる公開情報の一例は、図１４に示すように、（３，１）及び$E4\left(Skd2^{(3)}, KeyD^{(3)}\right)$である。ここで、（３，１）は、階層番号が３であり、ノード番号が１であることを示している。また、$E4\left(Skd2^{(3)}, KeyD^{(3)}\right)$は、$Skd2^{(3)}$を鍵として用いて、$KeyD^{(3)}$に暗号化アルゴリズムＥ４を施して得られる暗号文であることを示している。$KeyD^{(3)}$は、インデックス情報（３，１）で示されるノードに割り当てられるノード鍵であり、$Skd2^{(3)}$は、当該ノードの右下側に接続する下位ノードに割り当てられたノード鍵である。

【００９４】（２）木構造構築部５０４

木構造構築部５０４は、木構造構築部２０４と同様であるので、説明を省略する。

（３）制御部５０２

制御部５０２は、制御部２０２と同様であるので、説明を省略する。

【００９５】（４）ノード鍵生成部５０５

ノード鍵生成部５０５は、ＤＶＤ用木構造テーブル５１１の各ノード（リーフを除く）について、ノード鍵を生成し、生成したノード鍵を各ノードに対応付けて、ＤＶＤ用木構造テーブル５１１へ書き込む。なお、ノード鍵生成部５０５によるノード鍵の生成については、後述する。

【００９６】（５）公開簿生成部５０６

公開簿生成部５０６は、ＤＶＤ用公開簿５２１を生成し、生成したＤＶＤ用公開簿５２１を情報記憶部５０８に書き込み、生成したＤＶＤ用公開簿５２１を、公開簿供給装置７００へ送信する。なお、公開簿生成部５０６によるＤＶＤ用公開簿５２１の生成については、後述する。

【００９７】（６）送受信部５０７

送受信部５０７は、通信回線を介して、ＤＶＤ供給装置６００と接続され、また、インターネット５を介して、利用者機器１１００と接続されている。送受信部５０７は、制御部５０２とＤＶＤ供給装置６００との間で情報の送受信を行う。また、送受信部５０７は、制御部５０２と利用者機器１１００との間で情報の送受信を行う。

【００９８】（７）表示部５０１及び入力部５０３

表示部５０１は、制御部５０２の制御の元に各種の情報を表示する。また、入力部５０３は、ＤＶＤ供給システム管理装置５００の管理者からの情報の入力を受け付ける。

１．７　ＤＶＤ供給装置６００の構成

ＤＶＤ供給装置６００は、ＤＶＤ供給システム管理装置５００から受け取ったノード鍵を用いてグループ鍵を暗号化し、グループ鍵を用いて映画情報を暗号化し、暗号化グループ鍵及び暗号化映画情報を、ＤＶＤに書き込む。暗号化グループ鍵及び暗号化映画情報が書き込まれたＤＶＤは、利用者に供給される。利用者は、前記ＤＶＤを利用者機器１１００へ装着する。

【００９９】ＤＶＤ供給装置６００は、音楽コンテンツ配信装置３００と同様の構成を有しているので、ここでは、詳細の説明を省略する。

１．８　公開簿供給装置７００の構成

公開簿供給装置７００は、通信回線を介して、ＤＶＤ供給システム管理装置５００に接続されている。

【０１００】公開簿供給装置７００は、ＤＶＤ供給システム管理装置５００から通信回線を介して、ＤＶＤ用公開簿５２１を受信し、受信したＤＶＤ用公開簿５２１をＤＶＤに書き込む。ＤＶＤ用公開簿５２１が書き込まれたＤＶＤは、利用者に供給される。利用者は、前記ＤＶＤを利用者機器１１００へ装着する。

１．９　映画放送システム管理装置８００の構成

映画放送システム管理装置８００は、映画放送システム４において用いられる暗号化のための鍵を管理し、送信装置１０００及び放送衛星６を介して、後述する映画用公開簿を放送波により放送することにより、利用者機器１１００等に公開する。

【０１０１】映画放送システム管理装置８００は、図１５に示すように、表示部８０１、制御部８０２、入力部８０３、木構造構築部８０４、公開簿生成部８０６、送受信部８０７及び情報記憶部８０８から構成されている。映画放送システム管理装置８００は、鍵管理装置１００と同様のコンピュータシステムである。マイクロプ

ロセッサが、コンピュータプログラムに従って動作することにより、映画放送システム管理装置８００は、その機能を達成する。

【０１０２】（１）情報記憶部８０８

情報記憶部８０８は、映画放送用木構造テーブル８１１及び映画用公開簿８２１を有しており、また、初期値$x_0$８３１を予め記憶している。映画放送用木構造テーブル８１１は、図１６に一例として示す木構造Ｔ３００に対応しており、木構造Ｔ３００を表現するためのデータ構造を示している。

【０１０３】後述するように、木構造構築部８０４により、木構造Ｔ３００を表現するためのデータ構造が映画放送用木構造テーブル８１１として生成され、情報記憶部８０８に書き込まれる。

（木構造Ｔ３００）木構造Ｔ３００は、図１６に示すように、階層１から階層４までの４階層からなる２分木である。木構造Ｔ３００は、木構造Ｔ１００と同様の構造を有しているので、詳細の説明は、省略する。

【０１０４】ここで、木構造Ｔ３００に関連して複数の公開点が存在する。木構造Ｔ３００に含まれる２個のノード（同一の階層に属し、同一のノードの下位に接続する）にそれぞれ割り当てられた２個のノード鍵を、２次元空間（ｘ－ｙ座標系）上の２点とみなし、２点を通る直線上の１点が公開点である。公開点のｘ座標は、予め定められており、その値は、初期値x_0に等しい。

【０１０５】このように、公開点は、同一の階層に属するノードに割り当てられた２個のノード鍵に関連して求められる。具体的には、図１６に示すように、階層２に、関連して、１個の公開点ｓ７が存在し、階層３に、関連して、２個の公開点ｓ５、ｓ６が存在し、階層４に、関連して、４個の公開点ｓ１～ｓ４が存在する。公開点と階層との関係は、以下において、公開点は、ある階層に属すると表現することがある。

【０１０６】また、公開点は、インデックス情報（階層番号、公開点のノード番号）により示される。ここで、階層番号は、公開点が属する階層を示し、公開点のノード番号は、同一階層内において、公開点を識別するための識別番号である。

（映画放送用木構造テーブル８１１）映画放送用木構造テーブル８１１は、図１７に示すように、木構造Ｔ３００に含まれるノードと同じ数のノード情報を含んで構成されており、各ノード情報は、木構造Ｔ１００を構成する各ノードにそれぞれ対応している。

【０１０７】各ノード情報は、リーフを除くノードについては、階層番号、ノード番号及びノード鍵を含み、リーフについては、階層番号、ノード番号、ノード鍵及び機器ＩＤを含む。階層番号、ノード番号、ノード鍵及び機器ＩＤについては、上述したとおりであり、説明を省略する。

（映画用公開簿８２１）映画用公開簿８２１は、図２０に示すように、システムＩＤ、初期値x_0及び所定数個の公開情報を含んで構成されている。各公開情報は、インデックス情報及び公開点ｙ座標を含む。

【０１０８】ここで、前記所定数は、木構造Ｔ３００に関連して存在する公開点の数であり、木構造Ｔ３００に関連して存在する各公開点は、映画用公開簿８２１に含まれる各公開情報に対応している。システムＩＤは、上述したとおりであって、コンテンツを供給したり配信したりするコンテンツ供給システムを識別するための識別子である。

【０１０９】インデックス情報は、階層番号及び公開点のノード番号を含む。ここで、階層番号は、当該公開情報に対応する公開点が属する階層を示す番号である。また、公開点のノード番号は、各階層内において、公開点を識別する番号である。公開点ｙ座標は、公開点のｙ座標を示す。

（初期値x_0）初期値x_0は、各公開点のｘ座標を示す。

【０１１０】（２）木構造構築部８０４

木構造構築部８０４は、映画放送用木構造テーブル８１１を生成して情報記憶部８０８へ書き込む。具体的には、木構造構築部８０４は、木構造Ｔ３００に含まれる各ノードについて、階層番号とノード番号とを含むノード情報を生成し、生成したノード情報を映画放送用木構造テーブル８１１内に書き込む。なお、この時点では、各ノード情報には、ノード鍵及び機器ＩＤは、含まれていない。

【０１１１】木構造構築部８０４は、鍵管理装置１００から、制御部８０２を介して、機器ＩＤ及びシステム用機器鍵$Skdi^{(9)}$を受け取り、映画放送用木構造テーブル８１１において、受け取ったシステム用機器鍵$Skdi^{(9)}$が１個のリーフに対応するように、受け取った機器ＩＤ及びシステム用機器鍵$Skdi^{(9)}$を映画放送用木構造テーブル８１１に書き込む。また、前記リーフを示すリーフ番号を制御部８０２へ出力する。

【０１１２】（３）制御部８０２

制御部８０２は、機器ＩＤ及びシステム用機器鍵$Skdi^{(9)}$の受取りが終了するまで、機器ＩＤ及びシステム用機器鍵$Skdi^{(0)}$の受取りと、システム用機器鍵の映画放送用木構造テーブル８１１への書込みと、利用者機器へのリーフ番号の送信を繰り返す。

【０１１３】制御部８０２は、鍵管理装置１００から送受信部８０７を介して、機器ＩＤ及びシステム用機器鍵$Skdi^{(9)}$を受け取り、受け取った機器ＩＤ及びシステム用機器鍵$Skdi^{(9)}$を木構造構築部８０４へ出力する。また、制御部８０２は、木構造構築部８０４からリーフ番号を受け取り、送受信部８０７及びインターネット５を介して、受け取った機器ＩＤにより示される利用者機器へ、システムＩＤ（＝３）と受け取ったリーフ番号とを送信する。

【０１１４】さらに、制御部８０２は、映画放送用木構造テーブル８１１から、所定の基準に基づいて、１個のノード鍵を選択する。ここでは、一例として、リーフからルートへの経路上に存在する全てのノードのうち、最上位のノード即ちルートに割り当てられたノード鍵を選択する。次に、制御部８０２は、選択したノード鍵を、映画コンテンツ供給装置９００へ送信する。

【０１１５】（４）公開簿生成部８０６

公開簿生成部８０６は、映画用公開簿８２１を生成し、生成した映画用公開簿８２１を情報記憶部８０８に書き込み、生成した映画用公開簿８２１を、送信装置１０００へ送信する。また、公開簿生成部８０６は、木構造Ｔ３００に含まれる各ノード（リーフを除く）について、ノード鍵を生成し、ノードに割り当てる。

【０１１６】以下に、公開簿生成部８０６による映画用公開簿８２１の生成、ノード鍵の生成及びノードへの割り当てについて、説明する。公開簿生成部８０６は、システムＩＤ（ここでは、「３」）を映画用公開簿８２１へ書き込む。また、情報記憶部８０８から初期値 x_0 を読み出し、読み出した初期値 x_0 を映画用公開簿８２１へ書き込む。

【０１１７】次に、公開簿生成部８０６は、木構造Ｔ３００の、階層３から階層１まで順に、また、各階層内の各ノードについて順に、以下に示す処理・～・を繰り返す。

・公開簿生成部８０６は、当該ノードの下位に接続する２個の下位ノードに、それぞれ対応する２個のノード情報を映画放送用木構造テーブル８１１から読み出す。

【０１１８】ここで、一例として、当該ノードは、インデックス情報（３，１）により示されるノードＴ３０１であるとする。木構造Ｔ３００の一部分であって、Ｔ３０１を含むものを図１９に示す。公開簿生成部８０６は、ノードＴ３０１の下位に接続する２個の下位ノードＴ３０２、Ｔ３０３に、それぞれ対応する２個のノード情報８１２、８１３を映画放送用木構造テーブル８１１から読み出す。

【０１１９】・公開簿生成部８０６は、読み出した２個のノード情報からそれぞれ２個のノード鍵Ｎｋ１、Ｎｋ２を抽出する

ここで、一例として、公開簿生成部８０６は、読み出した２個のノード情報８１２、８１３から、ノード鍵Ｓｋｄ１$^{(0)}$、Ｓｋｄ２$^{(0)}$を抽出する。

・公開簿生成部８０６は、当該２個のノード鍵Ｎｋ１、Ｎｋ２をそれぞれ２個の点とみなし、２個の点を通る直線Ｌを求める。具体的には、ノード鍵Ｎｋ１が３２ビットで表現される場合に、Ｎｋ１の上位１６ビットをｘ座標とし、Ｎｋ１の下位１６ビットをｙ座標とし、これら（ｘ座標、ｙ座標）により２次元空間（ｘ－ｙ座標系）上の点を表現する。ノード鍵Ｎｋ２についても同様である。

【０１２０】ここで、一例として、公開簿生成部８０６は、ノード鍵Ｓｋｄ１$^{(0)}$、Ｓｋｄ２$^{(0)}$による２個の点を通る直線Ｌを求める。図１８に、ｘ－ｙ座標系上のノード鍵Ｓｋｄ１$^{(0)}$、Ｓｋｄ２$^{(0)}$による２個の点を示し、また、直線Ｌを示している。

・公開簿生成部８０６は、直線Ｌ上の点（x_0、$s_{(0)}$）を求める。

【０１２１】ここで、一例として、公開簿生成部８０６は、直線Ｌ上の点ｓ１（x_0、$s_{(1)}$）を求める。図１８に示すように、点ｓ１は、ノード鍵Ｓｋｄ１$^{(0)}$、Ｓｋｄ２$^{(0)}$による２個の点を通る直線Ｌ上に存在している。

・公開簿生成部８０６は、公開点ｙ座標 $s_{(0)}$ を、インデックス情報（階層番号、公開点のノード番号）とともに、映画用公開簿８２１へ書き込む。

【０１２２】ここで、一例として、公開簿生成部８０６は、インデックス情報（４，１）と公開点ｙ座標 $s_{1(0)}$ とを映画用公開簿８２１へ書き込む。

・公開簿生成部８０６は、直線Ｌのｙ切片ＹＩを求める。図１８に示すように、直線Ｌとｙ軸との交点のｙ座標は、ＹＩである。

・公開簿生成部８０６は、一方向性関数ｇを用いて、ｇ（ＹＩ）を算出する。

【０１２３】・公開簿生成部８０６は、ｇ（ＹＩ）をｘ座標とする直線Ｌ上の点のｙ座標ＹＧを求める。

・公開簿生成部８０６は、求めた点（ｇ（ＹＩ）、ＹＧ）をノード鍵とし、ノード鍵を当該ノードに対応付けて映画放送用木構造テーブル８１１へ書き込む。ここで、一例として、ＫｅｙＤ$^{(0)}$＝（ｇ（ＹＩ）、ＹＧ）である。

【０１２４】以上に厳明した処理・～・を繰り返すことにより、図１７に一例として示す映画放送用木構造テーブル８１１のノード（リーフを除く）に対して、ノード鍵が生成されて割り当てられ、また、図２０に一例として示す映画用公開簿８２１が生成される。

（５）送受信部８０７

送受信部８０７は、通信回線を介して、映画コンテンツ供給装置９００と接続され、また、通信回線を介して、送信装置１０００と接続されている。

【０１２５】送受信部８０７は、制御部８０２と映画コンテンツ供給装置９００との間で情報の送受信を行う。また、送受信部８０７は、制御部２０２から出力される情報を、送信装置１０００、送信用アンテナ１０、放送衛星６及び受信用アンテナ９を介して、利用者機器１１００へ送信する。

（６）表示部８０１及び入力部８０３

表示部８０１は、制御部８０２の制御の元に各種の情報を表示する。また、入力部８０３は、映画放送システム管理装置８００の管理者からの情報の入力を受け付ける。

【０１２６】１．１０　映画コンテンツ供給装置９００
映画コンテンツ供給装置９００は、映画放送システム管理装置８００から受け取ったノード鍵を用いてグループ鍵を暗号化し、グループ鍵を用いて映画情報を暗号化し、暗号化グループ鍵及び暗号化映画情報を、送信装置１０００、送信用アンテナ１０、放送衛星６、受信用アンテナ９を介して、利用者機器１１００へ送信する。

【０１２７】映画コンテンツ供給装置９００は、音楽コンテンツ配信装置３００と同様の構成を有しているので、ここでは、詳細の説明を省略する。

１．１１　送信装置１０００、放送衛星６
送信装置１０００は、それぞれ、映画放送システム管理装置８００及び映画コンテンツ供給装置９００と通信回線を介して接続されており、映画放送システム管理装置８００及び映画コンテンツ供給装置９００からそれぞれ情報を受け取り、受け取った情報を、送信用アンテナ１０により電波として放送衛星６へ送信する。

【０１２８】１．１２　利用者機器１１００
利用者機器１１００は、自身が記憶している機器鍵ｋｄｉ及び音楽用公開鍵に基づいて、暗号化音楽コンテンツを復号して、音楽コンテンツを再生し、自身が記憶している機器鍵ｋｄｉ及びＤＶＤ用公開鍵に基づいて、ＤＶＤに記録されている暗号化映画コンテンツを復号して、映画コンテンツを再生し、放送波を受信し、受信した放送波から暗号化映画コンテンツを抽出し、自身が記憶している機器鍵ｋｄｉ及び映画用公開鍵に基づいて、抽出した暗号化映画コンテンツを復号して、映画コンテンツを再生する。

【０１２９】利用者機器１１００は、図２１に示すように、情報記憶部１１０１、機器鍵記憶部１１０２、ノード鍵特定部１１０３、復号部１１０４、制御部１１０５、入力部１１０６、表示部１１０７、情報抽出部１１０８、復号部１１０９、送受信部１１１０、ＤＶＤ接続部１１１１、チューナ部１１１２及び再生部１１１３から構成されている。

【０１３０】利用者機器１１００には、受信用アンテナ９、モニタ１１１５及びスピーカ１１１６が接続されている。また、利用者機器１１００は、インターネット５に接続されている。なお、他の利用者機器については、利用者機器１１００と同様の構成を有しているので、説明を省略する。

【０１３１】（１）機器鍵記憶部１１０２
機器鍵記憶部１１０２は、機器鍵ｋｄｉ及び機器ＩＤを記憶するための領域を備えている。機器鍵ｋｄｉ及び機器ＩＤについては、上述した通りであるので、説明を省略する。

【０１３２】（２）情報記憶部１１０１、情報記憶部１１０１は、システムＩＤテーブル１１５１を有し、音楽用公開鍵１１６１、ＤＶＤ用公開鍵１１６２、映画用公開鍵１１６３、暗号化グループ鍵及び暗号化コンテンツを記憶するための領域を備えている。音楽用公開鍵、ＤＶＤ用公開鍵、映画用公開鍵、暗号化グループ鍵及び暗号化コンテンツについては、上述した通りであるので、説明を省略する。

【０１３３】システムＩＤテーブル１１５１は、システム名、システムＩＤ及びリーフ番号からなる組を複数個記憶するための領域を備えている。システム名は、音楽配信システム２、ＤＶＤ供給システム３及び映画放送システム４などのコンテンツ供給システムを特定するための名称である。システムＩＤは、上述したように、コンテンツ供給システムをシステムするために識別子である。

【０１３４】リーフ番号は、対応するコンテンツ供給システムにおいて、利用者機器１１００が割り当てられているリーフを示す番号である。

（３）送受信部１１１０、ＤＶＤ接続部１１１１、チューナ部１１１２
送受信部１１１０は、インターネット５と接続されており、外部の装置から情報を受信し、受け取った情報を情報抽出部１１０８へ出力する。

【０１３５】ＤＶＤ接続部１１１１は、利用者機器１１００に装着されたＤＶＤから情報を読み出し、読み出した情報を情報抽出部１１０８へ出力する。チューナ部１１１２は、受信用アンテナ９に接続されており、放送波を選択的に受信し、受信した放送波を情報として情報抽出部１１０８へ出力する。

（４）入力部１１０６、入力部１１０６は、利用者から情報の入力を受け付け、受け付けた情報を制御部１１０５へ出力する。

【０１３６】（５）制御部１１０５、制御部１１０５は、利用者から入力部１１０６を介して、利用するシステム名の入力を受け付ける。前記入力を受け付けると、制御部１１０５は、情報記憶部１１０１が有するシステムＩＤテーブル１１５１から、入力を受け付けたシステム名に対応するシステムＩＤを取得する。

【０１３７】次に、制御部１１０５は、取得したシステムＩＤが「１」、「２」又は「３」のいずれであるかを判断する。制御部１１０５は、システムＩＤが「１」であると判断する場合に、ノード鍵特定部１１０３に対して、ノード鍵の特定（１）の処理を行うように制御し、システムＩＤが「２」であると判断する場合に、ノード鍵特定部１１０３に対して、ノード鍵の特定（２）の処理を行うように制御し、システムＩＤが「３」であると判断する場合に、ノード鍵特定部１１０３に対して、ノード鍵の特定（３）の処理を行うように制御する。

【０１３８】制御部１１０５は、コンテンツの取得、復号、再生処理が終了したか否かを判断し、終了していないと判断する場合に、コンテンツの取得、復号、再生処理を繰り返すように、各構成要素を制御する。終了したと判断する場合に、制御部１１０５は、利用者機器１１

００によるコンテンツの取得、復号、再生を終了する。

【０１３９】（６）情報抽出部１１０８

（システムＩＤ及びリーフ番号の取得）情報抽出部１１０８は、音楽配信システム管理装置２００から、インターネット５及び送受信部１１１０を介して、システムＩＤ及びリーフ番号を受信し、受信したシステムＩＤ及びリーフ番号をシステム名「音楽配信システム」と対応付けて、システムＩＤテーブル１１５１へ書き込む。

【０１４０】また、情報抽出部１１０８は、ＤＶＤ供給システム管理装置５００から、インターネット５及び送受信部１１１０を介して、システムＩＤ及びリーフ番号を受信し、受信したシステムＩＤ及びリーフ番号をシステム名「ＤＶＤ供給システム」と対応付けて、システムＩＤテーブル１１５１へ書き込む。また、情報抽出部１１０８は、映画放送システム管理装置８００から、送信装置１０００、送信用アンテナ１０、放送衛星６、受信用アンテナ９及びチューナ部１１１２を介して、システムＩＤ及びリーフ番号を受信し、受信したシステムＩＤ及びリーフ番号をシステム名「映画放送システム」と対応付けて、システムＩＤテーブル１１５１へ書き込む。

【０１４１】（公開簿の取得）情報抽出部１１０８は、公開簿サーバ装置４００から、インターネット５及び送受信部１１１０を介して、音楽用公開簿を受信し、受信した音楽用公開簿を、音楽用公開簿１１６１として情報記憶部１１０１へ書き込む。また、利用者によりＤＶＤ用公開簿が記録されているＤＶＤが利用者機器１１００に装着されると、情報抽出部１１０８は、装着されたＤＶＤから、ＤＶＤ接続部１１１１を介して、ＤＶＤ用公開簿を読み出し、読み出したＤＶＤ用公開簿を、ＤＶＤ用公開簿１１６２として情報記憶部１１０１へ書き込む。

【０１４２】また、情報抽出部１１０８は、映画放送システム管理装置８００から、送信装置１０００、送信用アンテナ１０、放送衛星６、受信用アンテナ９及びチューナ部１１１２を介して、映画用公開簿を受信し、受信した映画用公開簿を、映画用公開簿１１６３として情報記憶部１１０１へ書き込む。

（暗号化グループ鍵及び暗号化コンテンツの取得）情報抽出部１１０８は、音楽コンテンツ配信装置３００から、インターネット５及び送受信部１１１０を介して、暗号化グループ鍵及び暗号化コンテンツを受信し、受信した暗号化グループ鍵及び暗号化コンテンツを、暗号化グループ鍵１１７１及び暗号化コンテンツ１１８１として、情報記憶部１１０１へ書き込む。

【０１４３】また、利用者により暗号化グループ鍵及び暗号化コンテンツが記録されているＤＶＤが利用者機器１１００に装着されると、情報抽出部１１０８は、装着されたＤＶＤから、ＤＶＤ接続部１１１１を介して、暗号化グループ鍵及び暗号化コンテンツを読み出し、読み出した暗号化グループ鍵及び暗号化コンテンツを、暗号化グループ鍵１１７１及び暗号化コンテンツ１１８１として、情報記憶部１１０１へ書き込む。

【０１４４】また、情報抽出部１１０８は、映画コンテンツ供給装置９００から、送信装置１０００、送信用アンテナ１０、放送衛星６、受信用アンテナ９及びチューナ部１１１２を介して、暗号化グループ鍵及び暗号化コンテンツを受信し、受信した暗号化グループ鍵及び暗号化コンテンツを、暗号化グループ鍵１１７１及び暗号化コンテンツ１１８１として、情報記憶部１１０１へ書き込む。

【０１４５】（７）復号部１１０４、ノード鍵特定部１１０３によるノード鍵の特定が終了すると、復号部１１０４は、情報記憶部１１０１から暗号化グループ鍵を読み出し、特定されたノード鍵を鍵として用いて、読み出した暗号化グループ鍵に復号アルゴリズムＤ３を施して、グループ鍵＝Ｄ３（ノード鍵、暗号化グループ鍵）を生成する。

【０１４６】ここで、復号アルゴリズムＤ３は、暗号化アルゴリズムＥ３に対応するものであって、暗号化アルゴリズムＥ３により生成された暗号文を復号する。

（８）復号部１１０９

復号部１１０９は、暗号化コンテンツを情報記憶部１１０１から読み出し、生成されたグループ鍵を鍵として用いて、読み出した暗号化コンテンツに復号アルゴリズムＤ２を施して、コンテンツ＝Ｄ２（グループ鍵、暗号化コンテンツ）を生成する。

【０１４７】ここで、復号アルゴリズムＤ２は、暗号化アルゴリズムＥ２に対応するものであって、暗号化アルゴリズムＥ２により生成された暗号文を復号する。

（９）再生部１１１３

再生部１１１３は、モニタ１１１５及びスピーカ１１１６に接続されている。再生部１１１３は、生成されたコンテンツを再生し、モニタ１１１５及びスピーカ１１１６に出力する。

【０１４８】（１０）表示部１１０７

表示部１１０７は、制御部１１０５の制御により、情報を表示する。

（１１）ノード鍵特定部１１０３

ノード鍵特定部１１０３は、制御部１１０５の制御により、次に示すノード鍵の特定（１）の処理、ノード鍵の特定（２）の処理及びノード鍵の特定（３）の処理のうちの何れかを実行する。

【０１４９】（ａ）ノード鍵の特定（１）の処理

ノード鍵特定部１１０３は、情報記憶部１１０１が有するシステムＩＤテーブル１１５１から、システムＩＤに対応するリーフ番号を読み出し、機器鍵記憶部１１０２から、機器鍵ｋｄｉを読み出す。また、ノード鍵特定部１１０３は、システムＩＤに対応する公開簿を特定する。公開簿に含まれているシステムＩＤと制御部１１０５により取得したシステムＩＤとが一致するか否かによ

り、公開簿を特定する。ここでは、システムＩＤは、「１」であるので、音楽用公開簿１１６１が特定される。

【０１５０】次に、ノード鍵特定部１１０３は、システム用機器鍵Ｓｋｄｉ$^{(0)}$＝ｈ（ｋｄｉ、システムＩＤ）を生成する。ここで、ｈは、一方向性関数である。次に、リーフ番号に、「１」を加算して、階層３のパス番号を求める。例えば、リーフ番号が「０００」である場合には、「０００」に「１」加算すると「００１」が得られる。この値は、リーフ番号「０００」が示すリーフが接続されるパスの番号と一致する。次に、ノード鍵特定部１１０３は、インデックス情報＝（３、パス番号）を設定し、音楽用公開簿１１６１から設定したインデックス情報に対応する暗号化ノード鍵を読み出す。次に、システム用機器鍵Ｓｋｄｉ$^{(0)}$　を鍵として用いて、読み出した暗号化ノード鍵を復号する。

【０１５１】

Ｒ$_{3}$＝Ｄ１（Ｓｋｄｉ$^{(0)}$　、暗号化ノード鍵）。

こうして、利用者機器１１００に割り当てられたリーフ番号が示すリーフの上側に接続するノードに割り当てられたノード鍵が求められる。以降同様にして、ノード鍵特定部１１０３は、さらに上位に接続するノードに割り当てられたノード鍵を求める。

【０１５２】このようにして、ノード鍵特定部１１０３は、リーフ番号が示すリーフからルートへの経路上の各ノードに割り当てられたノード鍵を求めることができる。次に、ノード鍵特定部１１０３は、このようにして、求めた複数のノード鍵のうちから１個のノード鍵を決定する。ここでは、最上位のノード、つまり、ルートに割り当てられたノード鍵を採用することとする。

【０１５３】（ｂ）ノード鍵の特定（２）の処理

ノード鍵特定部１１０３は、情報記憶部１１０１が有するシステムＩＤテーブル１１５１から、システムＩＤに対応するリーフ番号を読み出し、機器鍵記憶部１１０２から、機器鍵ｋｄｉを読み出す。また、ノード鍵特定部１１０３は、上記と同様にして、システムＩＤに対応する公開簿を特定する。ここでは、システムＩＤは、「２」であるので、ＤＶＤ用公開簿１１６２が特定される。

【０１５４】次に、ノード鍵特定部１１０３は、上記と同様にして、システム用機器鍵Ｓｋｄｉ$^{(0)}$　＝ｈ（ｋｄｉ、システムＩＤ）を生成する。次に、ノード鍵特定部１１０３は、木構造Ｔ２００の階層４から階層３へ、左パスをたどるか、右パスをたどるかをリーフ番号の最下位ビットの値により、決定する。最下位ビットの値が「０」であるなら、左パスをたどり、最下位ビットの値が「１」であるなら、右パスをたどる。

【０１５５】また、木構造Ｔ２００の階層３から階層２へ、左パスをたどるか、右パスをたどるかを決定する場合には、リーフ番号の第２ビットの値により、決定する。第２ビットの値が「０」であるなら、左パスをたどり、第２ビットの値が「１」であるなら、右パスをたどる。さらに、木構造Ｔ２００の階層２から階層１へ、左パスをたどるか、右パスをたどるかを決定する場合には、リーフ番号の最上位ビットの値により、決定する。最上位ビットの値が「０」であるなら、左パスをたどり、最上位ビットの値が「１」であるなら、右パスをたどる。

【０１５６】このように、リーフ番号の各ビットにより、左パスをたどるか、右パスをたどるかが決定できるのは、リーフ番号の各ビットが元々、左パスか又は右パスにより定められているからである。左パスをたどると決定する場合に、ノード鍵特定部１１０３は、ノード鍵Ｒ$_{3}$＝ｇ（Ｓｋｄｉ$^{(0)}$　）を求める。

【０１５７】右パスをたどると決定する場合に、ノード鍵特定部１１０３は、リーフ番号から階層３のノード番号を求め、インデックス情報＝（３、ノード番号）を設定し、ＤＶＤ用公開簿１１６２から、設定したインデックス情報に対応する暗号化ノード鍵を読み出し、読み出した暗号化ノード鍵を、Ｓｋｄｉ$^{(0)}$　を鍵として用いて、復号する。こうしてノード鍵Ｒ$_{3}$＝Ｄ４（Ｓｋｄｉ$^{(0)}$　、暗号化ノード鍵）が得られる。

【０１５８】ノード鍵特定部１１０３は、上に示した手順を、下位の階層から上位の階層へ向かって繰り返すことにより、リーフ番号により示されるリーフからルートへの経路上の各ノードに割り当てられたノード鍵を求める。次に、ノード鍵特定部１１０３は、このようにして、求めた複数のノード鍵のうちから１個のノード鍵を決定する。ここでは、最上位のノード、つまり、ルートに割り当てられたノード鍵を採用することとする。

【０１５９】（ｃ）ノード鍵の特定（３）の処理

ノード鍵特定部１１０３は、情報記憶部１１０１が有するシステムＩＤテーブル１１５１から、システムＩＤに対応するリーフ番号を読み出し、機器鍵記憶部１１０２から、機器鍵ｋｄｉを読み出し、システムＩＤに対応する公開簿を特定する。ここでは、システムＩＤは、「３」であるので、映画用公開簿１１６３が特定される。

【０１６０】次に、ノード鍵特定部１１０３は、システム用機器鍵Ｓｋｄｉ$^{(0)}$　＝ｈ（ｋｄｉ、システムＩＤ）を生成する。また、映画用公開簿１１６３から初期値ｘ$_{0}$を読み出す。次に、ノード鍵特定部１１０３は、リーフ番号から階層４の公開点のノード番号を求め、インデックス情報＝（４、公開点のノード番号）を設定し、設定したインデックス情報に対応する公開点ｙ$_{4}$座標ｙ$_{4}$を映画用公開簿１１６３から読み出す。次に、機器鍵ｋｄｉと公開点（ｘ$_{0}$、ｙ$_{4}$）を通る直線Ｌ$_{4}$を求め、直線Ｌ$_{4}$のｙ切片ＹＩ$_{4}$を求め、ｇ（ＹＩ$_{4}$）を求める。次に、ｇ（ＹＩ$_{4}$）をｘ座標とする直線Ｌ$_{4}$上の点のｙ座標ＹＧ$_{4}$を求め、Ｒ$_{3}$＝（ｇ（ＹＩ$_{4}$）、ＹＧ$_{4}$）とす

る。このようにしてノード鍵Ｒ₃が得られる。

【０１６１】ノード鍵特定部１１０３は、同様の手順を繰り返すことにより、リーフ番号により示されるリーフからルートへの経路上の各ノードに割り当てられたノード鍵を求める。次に、ノード鍵特定部１１０３は、このようにして、求めた複数のノード鍵のうちから１個のノード鍵を決定する。ここでは、最上位のノード、つまり、ルートに割り当てられたノード鍵を採用することとする。

【０１６２】１．１３　鍵管理装置１００の動作

鍵管理装置１００の動作について、図２２に示すフローチャートを用いて説明する。制御部１０２は、鍵管理業者から入力部１０１を介して、システムＩＤの入力を受け付け（ステップＳ１０１）、入力部１０１を介して、機器ＩＤの入力を受け付ける（ステップＳ１０２）。

【０１６３】次に、制御部１０２は、機器鍵管理テーブル１１１内に、入力を受け付けた前記機器ＩＤが記憶されているか否かを判断し、前記機器ＩＤが機器鍵管理テーブル１１１に記憶されていないと判断する場合に（ステップＳ１０３）、制御部１０２は、機器ＩＤを機器鍵生成部１０４へ出力し、機器鍵生成部１０４に対して機器鍵を新たに生成するように指示し、機器鍵生成部１０４は、新たに機器鍵ｋｄｉを生成し、機器ＩＤと生成した機器鍵ｋｄｉとを機器鍵出力部１０６へ出力し、生成した機器鍵ｋｄｉをシステム用機器鍵生成部１０５へ出力し、入力を受け付けた前記機器ＩＤと生成した機器鍵ｋｄｉとから構成される機器情報を機器鍵管理テーブル１１１へ書き込む（ステップＳ１０５）。

【０１６４】制御部１０２は、入力を受け付けた前記機器ＩＤが機器鍵管理テーブル１１１に記憶されていると判断する場合に（ステップＳ１０３）、機器鍵管理テーブル１１１から前記機器ＩＤを含む機器情報を読み出し、読み出した機器情報から機器鍵ｋｄｉを読み出し、読み出した機器鍵ｋｄｉをシステム用機器鍵生成部１０５へ出力する（ステップＳ１０４）。

【０１６５】システム用機器鍵生成部１０５は、機器鍵生成部１０４から機器鍵ｋｄｉを受け取り、制御部１０２からシステムＩＤを受け取り、受け取った機器鍵ｋｄｉとシステムＩＤとに一方向性関数ｈを施して、システム用機器鍵$Skdi^{(9)}$＝ｈ（ｋｄｉ、システムＩＤ）を生成し、生成したシステム用機器鍵$Skdi^{(9)}$とシステムＩＤとをシステム用機器鍵送信部１０８へ出力する（ステップＳ１０６）。

【０１６６】次に、システム用機器鍵生成部１０５は、機器ＩＤ、システムＩＤ及びシステム用機器鍵$Skdi^{(9)}$を対応付けて構成されるシステム情報をシステム用機器鍵管理テーブル１２１へ書き込む（ステップＳ１０７）。次に、機器鍵出力部１０６は、利用者機器に機器鍵が割り当てられていない場合に、機器ＩＤと機器鍵ｋｄｉとを製造装置１２００を介して利用者機器へ出力する（ステップＳ１０８）。

【０１６７】次に、システム用機器鍵送信部１０８は、システムＩＤにより示されるシステム用管理装置へ、機器ＩＤとシステム用機器鍵$Skdi^{(9)}$を送信する（ステップＳ１０９）。次に、機器鍵及びシステム用機器鍵の生成が終了しているならば（ステップＳ１１０）、鍵管理装置１００は、処理を終了し、終了していないならば（ステップＳ１１０）、ステップＳ１０１へ戻って処理を繰り返す。

【０１６８】１．１４　音楽配信システム管理装置２００の動作

（１）音楽配信システム管理装置２００の全体の動作

音楽配信システム管理装置２００の動作について、図２３に示すフローチャートを用いて説明する。木構造構築部２０４は、音楽配信用木構造テーブル２１１を生成して情報記憶部２０８へ書き込む（ステップＳ１２１）。

【０１６９】次に、制御部２０２は、鍵管理装置１００から送受信部２０７を介して、機器ＩＤ及びシステム用機器鍵$Skdi^{(9)}$を受け取り、受け取った機器ＩＤ及びシステム用機器鍵$Skdi^{(9)}$を木構造構築部２０４へ出力する（ステップＳ１２２）。次に、木構造構築部２０４は、音楽配信用木構造テーブル２１１において、受け取ったシステム用機器鍵$Skdi^{(9)}$が１個のリーフに対応するように、機器ＩＤ及びシステム用機器鍵$Skdi^{(9)}$を音楽配信用木構造テーブル２１１に書き込む（ステップＳ１２３）。次に、制御部２０２は、送受信部２０７及びインターネット５を介して、受け取った機器ＩＤにより示される利用者機器へ、システムＩＤ（＝１）とリーフ番号とを送信する（ステップＳ１２４）。

【０１７０】次に、制御部２０２は、機器ＩＤ及びシステム用機器鍵$Skdi^{(9)}$の受取りが終了したか否かを判断し、終了していないと判断する場合には（ステップＳ１２５）、ステップＳ１２２へ戻って処理を繰り返す。制御部２０２が、機器ＩＤ及びシステム用機器鍵$Skdi^{(9)}$の受取りが終了したと判断する場合には（ステップＳ１２５）、さらに、ノード鍵生成部２０５は、音楽配信用木構造テーブル２１１の各ノード（リーフを除く）について、ノード鍵を生成し、生成したノード鍵を各ノードに対応付けて、音楽配信用木構造テーブル２１１へ書き込む（ステップＳ１２６）。

【０１７１】次に、公開簿生成部２０６は、音楽用公開簿２２１を生成し、生成した音楽用公開簿２２１を情報記憶部２０８に書き込み（ステップＳ１２７）、生成した音楽用公開簿２２１を、公開簿サーバ装置４００へ送信し（ステップＳ１２８）、制御部２０２は、音楽配信用木構造テーブル２１１から、１個のノード鍵を選択し（ステップＳ１２９）、選択したノード鍵を、音楽コンテンツ配信装置３００へ送信する（ステップＳ１３０）。

【００１２】（２）音楽用公開簿の生成の動作
次に、公開簿生成部２０６による音楽用公開簿の生成の動作について、図２４～図２５に示すフローチャートを用いて説明する。なお、ここで説明する音楽用公開簿の生成の動作は、図２３に示すフローチャートにおけるステップＳ１２７の詳細である。
【００１３】公開簿生成部２０６は、システムＩＤ（ここでは、「１」）を音楽用公開簿２２１へ書き込む（ステップＳ１４１）。次に、ステップＳ１４２からステップＳ１５２において、階層３から階層１まで（階層の番号ｍ＝３、２、１）、順に、以下に示すステップＳ１４３～ステップＳ１５１を繰り返す。次に、公開簿生成部２０６は、ステップＳ１４３からステップＳ１５１において、階層番号ｍにより示される階層内の各ノードについて、順に、以下に示すステップＳ１４４～ステップＳ１５０を繰り返す。
【００１４】公開簿生成部２０６は、当該ノードに対応するノード情報を音楽配信用木構造テーブル２１１から読み出し（ステップＳ１４４）、読み出したノード情報からノード鍵Ｍｋを抽出する（ステップＳ１４５）。次に、公開簿生成部２０６は、当該ノードの直下に接続されている２個の下位ノードにそれぞれ対応する２個のノード情報を、音楽配信用木構造テーブル２１１から読み出し（ステップＳ１４６）、次に、読み出した２個のノード情報のそれぞれからノード鍵ｋ１、ｋ２を抽出する（ステップＳ１４７）。さらに、公開簿生成部２０６は、抽出したノード鍵ｋ１、ｋ２をそれぞれ鍵として用いて、ノード鍵Ｍｋに暗号化アルゴリズムＥ１を施して、暗号化ノード鍵Ｅ１（ｋ１，Ｍｋ）、Ｅ１（ｋ２，Ｍｋ）を生成し（ステップＳ１４８）、当該ノードから左下側への経路に対応するインデックス情報（階層番号、パス番号）と暗号化ノード鍵Ｅ１（ｋ１，Ｍｋ）とを、公開情報として、音楽用公開簿２２１へ書き込み（ステップＳ１４９）、当該ノードから右下側への経路に対応するインデックス情報（階層番号、パス番号）と暗号化ノード鍵Ｅ１（ｋ２，Ｍｋ）とを、公開情報として、音楽用公開簿２２１へ書き込む（ステップＳ１５０）。
【００１５】１．１５　音楽コンテンツ配信装置３００の動作
音楽コンテンツ配信装置３００の動作について、図２６に示すフローチャートを用いて説明する。ノード鍵取得部３０４は、音楽配信システム管理装置２００から、通信回線を介して、ノード鍵Ｎｋを受信し、受信したノード鍵Ｎｋを暗号化部３０５へ出力する（ステップＳ１７１）。次に、グループ鍵生成部３０２は、乱数を生成し、生成した乱数を用いて、グループ鍵Ｇを生成し、生成したグループ鍵Ｇを暗号化部３０５及び暗号化部３０３へ出力する（ステップＳ１７２）。次に、暗号化部３０５は、受け取ったノード鍵Ｎｋを用いて、受け取ったグループ鍵Ｇに暗号化アルゴリズムＥ３を施して、暗号化グループ鍵Ｅ３（Ｎｋ，Ｇ）を生成し、生成した暗号化グループ鍵Ｅ３（Ｎｋ，Ｇ）を送受信部３０６へ出力する（ステップＳ１７３）。
【００１６】次に、暗号化部３０３は、情報記憶部３０１から音楽情報ＭＣを読み出し（ステップＳ１７４）、グループ鍵生成部３０２からグループ鍵Ｇを受け取り、受け取ったグループ鍵Ｇを鍵として用いて、読み出した音楽情報ＭＣに暗号化アルゴリズムＥ２を施して、暗号化音楽情報Ｅ２（Ｇ，ＭＣ）を生成し、生成した暗号化音楽情報Ｅ２（Ｇ，ＭＣ）を送受信部３０６へ出力する（ステップＳ１７５）。
【００１７】次に、送受信部３０６は、暗号化グループ鍵Ｅ３（Ｎｋ，Ｇ）と暗号化音楽情報Ｅ２（Ｇ，ＭＣ）を受け取り、利用者の要求に応じて、受け取った暗号化グループ鍵Ｅ３（Ｎｋ，Ｇ）と暗号化音楽情報Ｅ２（Ｇ，ＭＣ）とを、インターネット５を介して、利用者機器１１００へ送信する（ステップＳ１７６）。
１．１６　ＤＶＤ供給システム管理装置５００の動作
（１）ＤＶＤ供給システム管理装置５００の全体の動作
ＤＶＤ供給システム管理装置５００の全体の動作について、図２７に示すフローチャートを用いて説明する。
【００１８】木構造構築部５０４は、ＤＶＤ用木構造テーブル５１１を生成して情報記憶部５０８へ書き込む（ステップＳ１９１）。次に、制御部５０２は、鍵管理装置１００から送受信部５０７を介して、機器ＩＤ及びシステム用機器鍵$Ｓｋｄｉ^{(2)}$を受け取り、受け取った機器ＩＤ及びシステム用機器鍵$Ｓｋｄｉ^{(2)}$を木構造構築部５０４へ出力する（ステップＳ１９２）。次に、木構造構築部５０４は、ＤＶＤ用木構造テーブル５１１において、受け取ったシステム用機器鍵$Ｓｋｄｉ^{(2)}$が１個のリーフに対応するように、機器ＩＤ及びシステム用機器鍵$Ｓｋｄｉ^{(2)}$をＤＶＤ用木構造テーブル５１１に書き込む（ステップＳ１９３）。次に、制御部５０２は、送受信部５０７及びインターネット５を介して、受け取った機器ＩＤにより示される利用者機器へ、システムＩＤ（＝２）とリーフ番号とを送信する（ステップＳ１９４）。
【００１９】次に、制御部５０２は、機器ＩＤ及びシステム用機器鍵$Ｓｋｄｉ^{(2)}$の受取りが終了したか否かを判断し、終了していないと判断する場合には（ステップＳ１９５）、ステップＳ１９２へ戻って処理を繰り返す。制御部５０２が、機器ＩＤ及びシステム用機器鍵$Ｓｋｄｉ^{(2)}$の受取りが終了したと判断する場合には（ステップＳ１９５）、さらに、ノード鍵生成部５０５は、ノード鍵を生成する（ステップＳ１９６）。
【００２０】次に、公開簿生成部５０６は、ＤＶＤ用公開簿５２１を生成し、生成したＤＶＤ用公開簿５２１を情報記憶部５０８に書き込み（ステップＳ１９７）、生成したＤＶＤ用公開簿５２１を、公開簿供給装置７００

へ送信し（ステップＳ１９８）、制御部５０２は、ＤＶＤ用木構造テーブル５１１から、１個のノード鍵を選択し（ステップＳ１９９）、選択したノード鍵を、ＤＶＤ供給装置６００へ送信する（ステップＳ２００）。

【０１８１】（２）ノード鍵の生成の動作

次に、ノード鍵生成部５０５によるノード鍵の生成の動作について、図２８に示すフローチャートを用いて説明する。なお、ここで説明するノード鍵の生成の動作は、図２７に示すフローチャートにおけるステップＳ１９６の詳細である。ノード鍵生成部５０５は、ステップＳ２１１からステップＳ２１８において、階層３から階層１まで（階層の番号ｍ＝３、２、１）、順に、以下に示すステップＳ２１２～ステップＳ２１７を繰り返す。

【０１８２】次に、ノード鍵生成部５０５は、ステップＳ２１２からステップＳ２１７において、階層番号ｍにより示される階層内の各ノードについて順に、以下に示すステップＳ２１３～ステップＳ２１６を繰り返す。ノード鍵生成部５０５は、当該ノードの下位に接続する２個の下位ノードのうち、左側に接続する下位ノードのノード情報をＤＶＤ用木構造テーブル５１１から読み出す（ステップＳ２１３）。

【０１８３】次に、ノード鍵生成部５０５は、読み出したノード情報からノード鍵を、ノード鍵Ｎｋとして抽出し（ステップＳ２１４）、次に、抽出したノード鍵Ｎｋに一方向性関数ｇを施して、新たなノード鍵Ｎｅｗ＝ｇ（ノード鍵Ｎｋ）を生成し（ステップＳ２１５）、新たに生成したノード鍵Ｎｅｗを、当該下位ノードに対応付けて、ＤＶＤ用木構造テーブル５１１へ書き込む（ステップＳ２１６）。

【０１８４】（３）ＤＶＤ用公開簿の生成の動作

次に、公開簿生成部５０６によるＤＶＤ用公開簿の生成の動作について、図２９～図３０に示すフローチャートを用いて説明する。なお、ここで説明するＤＶＤ用公開簿の生成の動作は、図２７に示すフローチャートにおけるステップＳ１９７の詳細である。

【０１８５】公開簿生成部５０６は、システムＩＤ（ここでは、「２」）をＤＶＤ用公開簿５２１へ書き込む（ステップＳ２３１）。次に、ステップＳ２３２からステップＳ２４１において、階層３から階層１まで（階層の番号ｍ＝３、２、１）、順に、以下に示すステップＳ２３３～ステップＳ２４０を繰り返す。次に、公開簿生成部５０６は、ステップＳ２３３からステップＳ２４０において、階層番号ｍにより示される階層内の各ノードについて順に、以下に示すステップＳ２３４～ステップＳ２３９を繰り返す。

【０１８６】公開簿生成部５０６は、当該ノードに対応するノード情報をＤＶＤ用木構造テーブル５１１から読み出し（ステップＳ２３４）、読み出したノード情報からノード鍵Ｍｋを抽出する（ステップＳ２３５）。次に、公開簿生成部５０６は、当該ノードの直下に接続されている２個の下位ノードのうち、右側の下位ノードのノード情報を、ＤＶＤ用木構造テーブル５１１から読み出し（ステップＳ２３６）、次に、読み出したノード情報からノード鍵ｋを抽出する（ステップＳ２３７）。さらに、公開簿生成部５０６は、抽出したノード鍵ｋを鍵として用いて、ノード鍵Ｍｋに暗号化アルゴリズムＥ４を施して、暗号化ノード鍵Ｅ４（ｋ，Ｍｋ）を生成し（ステップＳ２３８）、当該ノードに対応するインデックス情報（階層番号、ノード番号）と暗号化ノード鍵Ｅ４（ｋ，Ｍｋ）とを、公開情報として、ＤＶＤ用公開簿５２１へ書き込む（ステップＳ２３９）。

【０１８７】１．１７　映画放送システム管理装置８００の動作

映画放送システム管理装置８００の動作について、図３１～図３３に示すフローチャートを用いて説明する。木構造構築部８０４は、映画放送用木構造テーブル８１１を生成して情報記憶部８０８へ書き込む（ステップＳ２６１）。

【０１８８】次に、制御部８０２は、鍵管理装置１００から送受信部８０７を介して、機器ＩＤ及びシステム用機器鍵$Skdi^{(0)}$を受け取り、受け取った機器ＩＤ及びシステム用機器鍵$Skdi^{(0)}$を木構造構築部８０４へ出力する（ステップＳ２６２）。次に、木構造構築部８０４は、映画放送用木構造テーブル８１１において、受け取ったシステム用機器鍵$Skdi^{(0)}$が１個のリーフに対応するように、機器ＩＤ及びシステム用機器鍵$Skdi^{(0)}$を映画放送用木構造テーブル８１１に書き込む（ステップＳ２６３）。次に、制御部８０２は、送受信部８０７及びインターネット５を介して、受け取った機器ＩＤにより示される利用者機器へ、システムＩＤ（＝３）とリーフ番号とを送信する（ステップＳ２６４）。

【０１８９】次に、制御部８０２は、機器ＩＤ及びシステム用機器鍵$Skdi^{(0)}$の受取りが終了したか否かを判断し、終了していないと判断する場合には（ステップＳ２６５）、ステップＳ２６２へ戻って処理を繰り返す。制御部８０２が、機器ＩＤ及びシステム用機器鍵$Skdi^{(0)}$の受取りが終了したと判断する場合には（ステップＳ２６５）、公開簿生成部８０６は、システムＩＤ（ここでは、「３」）を映画用公開簿８２１へ書き込み（ステップＳ２６６）、情報記憶部８０８から初期値x_0を読み出し（ステップＳ２６７）、読み出した初期値x_0を映画用公開簿８２１へ書き込む（ステップＳ２６８）。

【０１９０】次に、公開簿生成部８０６は、ステップＳ２６９からステップＳ２８１において、階層３から階層１まで（階層の番号ｍ＝３、２、１）順に、以下に示すステップＳ２７０～ステップＳ２８０を繰り返す。次に、公開簿生成部８０６は、ステップＳ２７０からステップＳ２８０において、階層番号ｍにより示される階層

内の各ノードについて順に、以下に示すステップＳ２７１～ステップＳ２７９を繰り返す。

【０１９１】公開簿生成部８０６は、当該ノードの下位に接続する２個の下位ノードに、それぞれ対応する２個のノード情報を映画放送用木構造テーブル８１１から読み出し（ステップＳ２７１）、読み出した２個のノード情報からそれぞれ２個のノード鍵Ｎｋ１、Ｎｋ２を抽出する（ステップＳ２７２）。次に、公開簿生成部８０６は、当該２個のノード鍵Ｎｋ１、Ｎｋ２をそれぞれ２個の点とみなし、２個の点を通る直線Ｌを求め（ステップＳ２７３）、直線Ｌ上の点（x_0、s_ω　）を求め（ステップＳ２７４）、公開点ｙ座標s_ω　を映画用公開簿８２１へ書き込む（ステップＳ２７５）。次に、公開簿生成部８０６は、直線Ｌのｙ切片ＹＩを求め（ステップＳ２７６）、一方向性関数ｇを用いて、ｇ（ＹＩ）を算出し（ステップＳ２７７）、ｇ（ＹＩ）をｘ座標とする直線Ｌ上の点のｙ座標ＹＧを求め（ステップＳ２７８）、求めた点（ｇ（ＹＩ）、ＹＧ）をノード鍵とし、ノード鍵を当該ノードに対応付けて映画放送用木構造テーブル８１１へ書き込む（ステップＳ２８０）。

【０１９２】ステップＳ２６９からステップＳ２８１における各階層についての繰り返しが終了すると、制御部８０２は、送受信部８０７を介して、生成した映画用公開簿８２１を、送信装置１０００へ送信し、送信装置１０００は、放送衛星６を介して、映画用公開簿８２１を放送波に載せて放送する（ステップＳ２８２）。制御部８０２は、映画放送用木構造テーブル８１１から、１個のノード鍵を選択し（ステップＳ２８３）、選択したノード鍵を、映画コンテンツ供給装置９００へ送信する（ステップＳ２８４）。

【０１９３】１．１８　利用者機器１１００の動作

（１）利用者機器１１００全体の動作

利用者機器１１００全体の動作について、図３４に示すフローチャートを用いて説明する。情報抽出部１１０８は、音楽配信システム管理装置２００から、インターネット５及び送受信部１１１０を介して、システムＩＤ及びリーフ番号を受信し、受信したシステムＩＤ及びリーフ番号をシステム名「音楽配信システム」と対応付けて、ステップＳ１１５１へ書き込む。また、情報抽出部１１０８は、ＤＶＤ供給システム管理装置５００から、インターネット５及び送受信部１１１０を介して、システムＩＤ及びリーフ番号を受信し、受信したシステムＩＤ及びリーフ番号をシステム名「ＤＶＤ供給システム」と対応付けて、システムＩＤテーブル１１５１へ書き込む。また、情報抽出部１１０８は、映画放送システム管理装置８００から、送信装置１０００、送信用アンテナ１０、放送衛星６、受信用アンテナ９及びチューナ部１１１２を介して、システムＩＤ及びリーフ番号を受信し、受信したシステムＩＤ及びリーフ番号をシステム名「映画放送システム」と対応付けて、システムＩＤテーブル１１５１へ書き込む（ステップＳ３０１）。

【０１９４】次に、情報抽出部１１０８は、公開簿サーバ装置４００から、インターネット５及び送受信部１１１０を介して、音楽用公開簿を受信し、受信した音楽用公開簿を、音楽用公開簿１１６１として情報記憶部１１０１へ書き込む。また、利用者によりＤＶＤ用公開簿が記録されているＤＶＤが利用者機器１１００に装着されると、情報抽出部１１０８は、装着されたＤＶＤから、ＤＶＤ接続部１１１１を介して、ＤＶＤ用公開簿を読み出し、読み出したＤＶＤ用公開簿を、ＤＶＤ用公開簿１１６２として情報記憶部１１０１へ書き込む。また、情報抽出部１１０８は、映画放送システム管理装置８００から、送信装置１０００、送信用アンテナ１０、放送衛星６、受信用アンテナ９及びチューナ部１１１２を介して、映画用公開簿を受信し、受信した映画用公開簿を、映画用公開簿１１６３として情報記憶部１１０１へ書き込む（ステップＳ３０２）。

【０１９５】次に、制御部１１０５は、利用者から入力部１１０６を介して、利用するシステム名の入力を受け付け（ステップＳ３０３）、情報記憶部１１０１が有するシステムＩＤテーブル１１５１から、入力を受け付けたシステム名に対応するシステムＩＤを取得する（ステップＳ３０４）。次に、情報抽出部１１０８は、音楽コンテンツ配信装置３００から、インターネット５及び送受信部１１１０を介して、暗号化グループ鍵及び暗号化コンテンツを受信し、受信した暗号化グループ鍵及び暗号化コンテンツを、暗号化グループ鍵１１７１及び暗号化コンテンツ１１８１として、情報記憶部１１０１へ書き込む。又は、利用者により暗号化グループ鍵及び暗号化コンテンツが記録されているＤＶＤが利用者機器１１００に装着されると、情報抽出部１１０８は、装着されたＤＶＤから、ＤＶＤ接続部１１１１を介して、暗号化グループ鍵及び暗号化コンテンツを読み出し、読み出した暗号化グループ鍵及び暗号化コンテンツを、暗号化グループ鍵１１７１及び暗号化コンテンツ１１８１として、情報記憶部１１０１へ書き込む。又は、情報抽出部１１０８は、映画コンテンツ供給装置９００から、送信装置１０００、送信用アンテナ１０、放送衛星６、受信用アンテナ９及びチューナ部１１１２を介して、暗号化グループ鍵及び暗号化コンテンツを受信し、受信した暗号化グループ鍵及び暗号化コンテンツを、暗号化グループ鍵１１７１及び暗号化コンテンツ１１８１として、情報記憶部１１０１へ書き込む（ステップＳ３０５）。

【０１９６】次に、制御部１１０５は、システムＩＤが「１」、「２」又は「３」のいずれであるかを判断し、システムＩＤが「１」であると判断する場合に（ステップＳ３０６）、ノード鍵特定部１１０３は、ノード鍵の特定（１）の処理を行う（ステップＳ３０７）。システムＩＤが「２」であると判断する場合に（ステップＳ３

０６）、ノード鍵特定部１１０３は、ノード鍵の特定（２）の処理を行う（ステップＳ３０８）。システムＩＤが「３」であると判断する場合に（ステップＳ３０６）、ノード鍵特定部１１０３は、ノード鍵の特定（３）の処理を行う（ステップＳ３０９）。

【０１９７】ノード鍵特定部１１０３によるノード鍵の特定が終了すると、復号部１１０４は、情報記憶部１１０１から暗号化グループ鍵を読み出し、特定されたノード鍵を鍵として用いて、読み出した暗号化グループ鍵を復号して、グループ鍵Ｄ３（ノード鍵、暗号化グループ鍵）を生成する（ステップＳ３１０）。次に、復号部１１０９は、暗号化コンテンツを情報記憶部１１０１から読み出し、生成されたグループ鍵を鍵として用いて、読み出した暗号化コンテンツを復号して、コンテンツＤ２（グループ鍵、暗号化コンテンツ）を生成する（ステップＳ３１１）。

【０１９８】次に、再生部１１１３は、生成されたコンテンツを再生して出力する（ステップＳ３１２）。次に、制御部１１０５は、コンテンツの復号処理が終了したか否かを判断し、終了していないと判断する場合に（ステップＳ３１３）、ステップＳ３０３へ戻って、処理を繰り返す。終了したと判断する場合に（ステップＳ３１３）、制御部１１０５は、利用者機器１１００によるコンテンツの復号、再生を終了する。

【０１９９】（２）ノード鍵の特定（１）の動作

ノード鍵特定部１１０３によるノード鍵の特定（１）の動作について、図３５～図３６に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図３４のフローチャートのステップＳ３０７の詳細である。ノード鍵特定部１１０３は、情報記憶部１１０１が有するシステムＩＤテーブル１１５１から、システムＩＤに対応するリーフ番号を読み出し（ステップＳ３２１）、機器鍵記憶部１１０２から、機器鍵ｋｄｉを読み出し（ステップＳ３２２）、システムＩＤに対応する公開簿を特定する。ここでは、システムＩＤは、「１」であるので、音楽用公開簿１１６１が特定される（ステップＳ３２３）。

【０２００】次に、ノード鍵特定部１１０３は、システム用機器鍵$Skdi^{(2)}$＝ｈ（ｋｄｉ、システムＩＤ）を生成し（ステップＳ３２４）、リーフ番号から階層３のパス番号を求め（ステップＳ３２５）、インデックス情報＝（３、パス番号）を設定し（ステップＳ３２６）、音楽用公開簿１１６１から設定したインデックス情報に対応する暗号化ノード鍵を読み出し（ステップＳ３２７）、次に、システム用機器鍵$Skdi^{(2)}$　を鍵として用いて、読み出した暗号化ノード鍵を復号する。R_3＝Ｄ１（$Skdi^{(2)}$　、暗号化ノード鍵）（ステップＳ３２８）。

【０２０１】次に、ノード鍵特定部１１０３は、リーフ番号から階層２のパス番号を求め（ステップＳ３２９）、インデックス情報＝（２、パス番号）を設定し（ステップＳ３３０）、音楽用公開簿１１６１から設定したインデックス情報に対応する暗号化ノード鍵を読み出し（ステップＳ３３１）、R_3 を鍵として用いて、読み出した暗号化ノード鍵を復号する。R_2＝Ｄ１（R_3 、暗号化ノード鍵）（ステップＳ３３２）。

【０２０２】次に、ノード鍵特定部１１０３は、インデックス情報＝（１、１）を設定し（ステップＳ３３３）、音楽用公開簿１１６１から設定したインデックス情報に対応する暗号化ノード鍵を読み出し（ステップＳ３３４）、R_2 を鍵として用いて、読み出した暗号化ノード鍵を復号する。R_1＝Ｄ１（R_2 、暗号化ノード鍵）（ステップＳ３３５）。

【０２０３】次に、ノード鍵特定部１１０３は、$Skdi^{(0)}$ 、R_3 、R_2 、R_1 のうちから１個のノード鍵を決定する（ステップＳ３３６）。

（３）ノード鍵の特定（２）の動作

ノード鍵特定部１１０３によるノード鍵の特定（２）の動作について、図３７～図４０に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図３４のフローチャートのステップＳ３０８の詳細である。

【０２０４】ノード鍵特定部１１０３は、情報記憶部１１０１が有するシステムＩＤテーブル１１５１から、システムＩＤに対応するリーフ番号を読み出し（ステップＳ３５１）、機器鍵記憶部１１０２から、機器鍵ｋｄｉを読み出し（ステップＳ３５２）、システムＩＤに対応する公開簿を特定する。ここでは、システムＩＤは、「２」であるので、ＤＶＤ用公開簿１１６２が特定される（ステップＳ３５３）。

【０２０５】次に、ノード鍵特定部１１０３は、システム用機器鍵$Skdi^{(2)}$＝ｈ（ｋｄｉ、システムＩＤ）を生成する（ステップＳ３５４）。次に、ノード鍵特定部１１０３は、木構造Ｔ２００の階層４から階層３へ、左パスをたどるか、右パスをたどるかをリーフ番号により、決定する（ステップＳ３５５）左パスをたどると決定する場合に（ステップＳ３５６）、ノード鍵特定部１１０３は、R_3＝ｇ（$Skdi^{(2)}$　）を求める（ステップＳ３５７）。右パスをたどると決定する場合に（ステップＳ３５６）、ノード鍵特定部１１０３は、リーフ番号から階層３のノード番号を求め（ステップＳ３５８）、インデックス情報＝（３、ノード番号）を設定し（ステップＳ３５９）、ＤＶＤ用公開簿１１６２から、設定したインデックス情報に対応する暗号化ノード鍵を読み出し（ステップＳ３６０）、読み出した暗号化ノード鍵を、$Skdi^{(2)}$　を鍵として用いて、復号する。R_3＝Ｄ４（$Skdi^{(2)}$　、暗号化ノード鍵）（ステップＳ３６１）。

【０２０６】次に、ノード鍵特定部１１０３は、木構造Ｔ２００の階層３から階層２へ、左パスをたどるか、右パスをたどるかをリーフ番号により、決定する（ステッ

プＳ３６２）。左パスをたどると決定する場合に（ステップＳ３６３）、ノード鍵特定部１１０３は、R_2＝ｇ（R_3）を求める（ステップＳ３６４）。右パスをたどると決定する場合に（ステップＳ３６３）、ノード鍵特定部１１０３は、リーフ番号から階層２のノード番号を求め（ステップＳ３６５）、インデックス情報＝（２、ノード番号）を設定し（ステップＳ３６６）、ＤＶＤ用公開簿１１６２から、設定したインデックス情報に対応する暗号化ノード鍵を読み出し（ステップＳ３６７）、読み出した暗号化ノード鍵を、R_3 を鍵として用いて、復号する。R_3 ＝Ｄ４（R_3 ，暗号化ノード鍵）（ステップＳ３６８）。

【０２０７】次に、ノード鍵特定部１１０３は、木構造Ｔ２００の階層２から階層１へ、左パスをたどるか、右パスをたどるかをリーフ番号により、決定する（ステップＳ３６９）。左パスをたどると決定する場合に（ステップＳ３７０）、ノード鍵特定部１１０３は、R_1 ＝ｇ（R_1）を求める（ステップＳ３７１）。右パスをたどると決定する場合に（ステップＳ３７０）、ノード鍵特定部１１０３は、インデックス情報＝（１、１）を設定し（ステップＳ３７２）、ＤＶＤ用公開簿１１６２から、設定したインデックス情報に対応する暗号化ノード鍵を読み出し（ステップＳ３７３）、読み出した暗号化ノード鍵を、R_2 を鍵として用いて、復号する。R_1 ＝Ｄ４（R_2 ，暗号化ノード鍵）　（ステップＳ３７４）。

【０２０８】次に、ノード鍵特定部１１０３は、$Skd_i^{(2)}$ 、R_3 、R_2 、R_1 、R_1 のうちから１個のノード鍵を決定する（ステップＳ３７５）。

（４）ノード鍵の特定（３）の動作

ノード鍵特定部１１０３によるノード鍵の特定（３）の動作について、図４１～図４３に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図３４のフローチャートのステップＳ３０９の詳細である。

【０２０９】ノード鍵特定部１１０３は、情報記憶部１１０１が有するシステムＩＤテーブル１１５１から、システムＩＤに対応するリーフ番号を読み出し（ステップＳ３９１）、機器鍵記憶部１１０２から、機器鍵k_{di}を読み出し（ステップＳ３９２）、システムＩＤに対応する公開簿を特定する。ここでは、システムＩＤは、「３」であるので、映画用公開簿１１６３が特定される（ステップＳ３９３）。

【０２１０】次に、ノード鍵特定部１１０３は、システム用機器鍵$Skd_i^{(3)}$ ＝ｈ（k_{di} 、システムＩＤ）を生成し（ステップＳ３９４）、映画用公開簿１１６３から初期値x_0 を読み出す（ステップＳ３９５）。次に、ノード鍵特定部１１０３は、リーフ番号から階層４の公開点のノード番号を求め（ステップＳ３９６）、インデックス情報＝（４、公開点のノード番号）を設定し（ステップＳ３９７）、設定したインデックス情報に対応する公開点ｙ座標y_4 を映画用公開簿１１６３から読み出し（ステップＳ３９８）、機器鍵k_{di}と公開点（x_0 、y_4 ）を通る直線L_4 を求め（ステップＳ３９９）、直線L_4 のｙ切片Y_{I4} を求め（ステップＳ４００）、ｇ（Y_{I4} ）を求め（ステップＳ４０１）、ｇ（Y_{I4} ）をｘ座標とする直線L_4 上の点のｙ座標YG_4 を求め、R_3 ＝（ｇ（Y_{I4} ）、YG_4 ）とする（ステップＳ４０２）。

【０２１１】次に、ノード鍵特定部１１０３は、リーフ番号から階層３の公開点のノード番号を求め（ステップＳ４０３）、インデックス情報＝（３、公開点のノード番号）を設定し（ステップＳ４０４）、設定したインデックス情報に対応する公開点ｙ座標y_3 を映画用公開簿１１６３から読み出し（ステップＳ４０５）、求めたR_3 と公開点（x_0 、y_3 ）を通る直線L_3 を求め（ステップＳ４０６）、直線L_3 のｙ切片Y_{I3} を求め（ステップＳ４０７）、ｇ（Y_{I3} ）を求め（ステップＳ４０８）、ｇ（Y_{I3} ）をｘ座標とする直線L_3 上の点のｙ座標YG_3 を求め、R_2 ＝（ｇ（Y_{I3} ）、YG_3 ）とする（ステップＳ４０９）。

【０２１２】次に、ノード鍵特定部１１０３は、リーフ番号から階層２の公開点のノード番号を求め（ステップＳ４１０）、インデックス情報＝（２、公開点のノード番号）を設定し（ステップＳ４１１）、設定したインデックス情報に対応する公開点ｙ座標y_2 を映画用公開簿１１６３から読み出し（ステップＳ４１２）、求めたR_2 と公開点（x_0 、y_2 ）を通る直線L_2 を求め（ステップＳ４１３）、直線L_2 のｙ切片Y_{I2} を求め（ステップＳ４１４）、ｇ（Y_{I2} ）を求め（ステップＳ４１５）、ｇ（Y_{I2} ）をｘ座標とする直線L_2 上の点のｙ座標YG_2 を求め、R_1 ＝（ｇ（Y_{I2} ）、YG_2 ）とする（ステップＳ４１６）。

【０２１３】次に、ノード鍵特定部１１０３は、$Skd_i^{(0)}$ 、R_2 、R_2 、R_1 のうちから１個のノード鍵を決定する（ステップＳ４１７）。

２．その他の変形例

音楽配信システム管理装置２００及び利用者機器１１００の変形例である音楽配信システム管理装置２００ｂ及び利用者機器１１００ｂ（これらについては図示していない）について説明する。なお、ここでは、音楽配信システム管理装置２００及び利用者機器１１００との相違点を中心として説明する。

【０２１４】２．１　音楽配信システム管理装置２００ｂの構成

変形例としての音楽配信システム管理装置２００ｂは、音楽配信システム管理装置２００と同様に、音楽配信システム２において用いられる暗号化のための鍵を管理し、暗号化のためのノード鍵を音楽コンテンツ配信装置３００へ出力し、また音楽用公開簿を公開簿サーバ装置４００を介して、利用者機器１１００ｂに公開する。し

かしながら、音楽配信システム管理装置２００ｂは、上記の暗号化のための鍵の管理管理方法及び音楽用公開簿の作成方法において、音楽配信システム管理装置２００と相違する。

【０２１５】音楽配信システム管理装置２００ｂは、音楽配信システム管理装置２００と同様に、表示部２０１ｂ、制御部２０２ｂ、入力部２０３ｂ、木構造構築部２０４ｂ、公開簿生成部２０６ｂ、送受信部２０７ｂ及び情報記憶部２０８ｂから構成されている。音楽配信システム管理装置２００ｂは、音楽配信システム管理装置２００と同様のコンピュータシステムである。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、音楽配信システム管理装置２００ｂは、その機能を達成する。

【０２１６】（１）情報記憶部２０８ｂ

情報記憶部２０８ｂは、音楽配信用木構造テーブル２１１ｂ及び音楽用公開簿２２１ｂを有している。音楽配信用木構造テーブル２１１ｂは、図４４に一例として示す木構造Ｔ４００に対応しており、木構造Ｔ４００を表現するためのデータ構造を示している。

【０２１７】後述するように、木構造構築部２０４ｂにより、木構造Ｔ４００を表現するためのデータ構造が音楽配信用木構造テーブル２１１ｂとして生成され、情報記憶部２０８ｂに書き込まれる。

（木構造Ｔ４００）木構造Ｔ４００は、図４４に示すように、階層１から階層４までの４階層からなる２分木である。木構造Ｔ４００は、木構造Ｔ１００と同様の構造を有しているので、詳細の説明は、省略する。

【０２１８】（音楽配信用木構造テーブル２１１ｂ）音楽配信用木構造テーブル２１１ｂは、図４５に示すように、木構造Ｔ４００に含まれるノードと同じ数のノード情報を含んで構成されており、各ノード情報は、木構造Ｔ４００を構成する各ノードにそれぞれ対応している。ルートに対応するノード情報は、階層番号、ノード番号及びノード鍵を含む。また、ルート及びリーフを除くノードに対応するノード情報は、階層番号、ノード番号、ノード鍵及びパス情報を含む。また、リーフに対応するノード情報は、階層番号、ノード番号、ノード鍵及び機器ＩＤを含む。

【０２１９】階層番号、ノード番号、ノード鍵及び機器ＩＤについては、上述した通りであるので、説明を省略する。パス情報は、対応する階層番号及びノード番号により示されるノードから、上位のノードへ至るパスに一意に割り当てられた情報であり、乱数を用いて生成されたものである。ここで、対応する階層番号及びノード番号とは、当該パス情報を含むノード情報に含まれる階層番号及びノード番号を指す。なお、パス情報は、当該パスに一意に割り当てられた番号であるとしてもよい。

【０２２０】（音楽用公開簿２２１ｂ）音楽用公開簿２２１ｂは、図４６に示すように、システムＩＤ、公開鍵、第１所定数個のパス公開情報及び第２所定数個のノード鍵公開情報を含んで構成されている。システムＩＤは、上述したとおりであって、コンテンツを供給したり配信したりするコンテンツ供給システムを識別するための識別子である。

【０２２１】公開鍵は、ＲＳＡ公開鍵暗号方式に基づいて生成され、整数ｅ及び整数ｎを含む。整数ｅ及び整数ｎについては、後述する。前記第１所定数は、木構造Ｔ４００において、木構造Ｔ４００に含まれる各ノード（ルート及びリーフを除く）から上位のノードへ至るパスの数である。各パス公開情報は、インデックス情報及びパス情報を含み、インデックス情報は、階層番号及びパス番号を含む。階層番号、パス番号及びパス情報については、上述したとおりであるので、説明を省略する。

【０２２２】前記第２所定数は、木構造Ｔ４００において、木構造Ｔ４００に含まれる各リーフから上位のノードへ至るパスの数である。各ノード鍵公開情報は、インデックス情報及び暗号化ノード鍵を含み、インデックス情報は、階層番号及びパス番号を含む。階層番号及びパス番号については、上述したとおりであるので、説明を省略する。暗号化ノード鍵は、対応するノードに割り当てられたノード鍵に、対応するパス番号により示されるパスにより接続される下位ノードに割り当てられたノード鍵を鍵として、暗号化アルゴリズムＥ１を施して生成されたものである。

【０２２３】音楽用公開簿２２１ｂに含まれるパス公開情報の一例は、図４６に示すように、（１、１）及びP_1を含む。ここで、（１、１）は、階層番号が１であり、パス番号が１であることを示している。また、P_1は、パス情報である。また、音楽用公開簿２２１ｂに含まれるノード鍵公開情報の一例は、図４６に示すように、（３、１）及び$E1(Skd1^{(0)}, Key D^{(0)})$を含む。ここで、（３、１）は、階層番号が３であり、パス番号が１であることを示している。また、$E1(Skd1^{(0)}, KeyD^{(0)})$は、$Skd1^{(0)}$を鍵として用いて、$KeyD^{(0)}$に暗号化アルゴリズムＥ１を施して得られる暗号文であることを示している。

【０２２４】（２）木構造構築部２０４ｂ

木構造構築部２０４ｂは、音楽配信用木構造テーブル２１１ｂを生成して情報記憶部２０８へ書き込む。具体的には、木構造構築部２０４ｂは、木構造Ｔ４００に含まれる各ノードについて、階層番号とノード番号とを含むノード情報を生成し、生成したノード情報を音楽配信用木構造テーブル２１１ｂ内に書き込む。なお、この時点では、各ノード情報には、ノード鍵、機器ＩＤ及びパス情報は、含まれていない。

【０２２５】木構造構築部２０４ｂは、鍵管理装置１００から、制御部２０２ｂを介して、機器ＩＤ及びシステム用機器鍵$Skd_i^{(0)}$を受け取り、音楽配信用木構造テーブル２１１ｂにおいて、受け取ったシステム用機器

鍵Ｓｋｄｉ$^{(i)}$　がｉ個のリーフに対応するように、受け取った機器ＩＤ及びシステム用機器鍵Ｓｋｄｉ$^{(i)}$　を音楽配信用木構造テーブル２１１ｂに書き込む。また、前記リーフを示すリーフ番号を制御部２０２ｂへ出力する。

【０２２６】（３）制御部２０２ｂ

制御部２０２ｂは、機器ＩＤ及びシステム用機器鍵Ｓｋｄｉ$^{(i)}$　の受取りが終了するまで、機器ＩＤ及びシステム用機器鍵Ｓｋｄｉ$^{(i)}$　の受取りと、システム用機器鍵の音楽配信用木構造テーブル２１１ｂへの書込みと、利用者機器へのリーフ番号の送信とを繰り返すように制御する。

【０２２７】次に、制御部２０２ｂは、鍵管理装置１００から送受信部２０７ｂを介して、機器ＩＤ及びシステム用機器鍵Ｓｋｄｉ$^{(i)}$　を受け取り、受け取った機器ＩＤ及びシステム用機器鍵Ｓｋｄｉ$^{(i)}$　を木構造構築部２０４ｂへ出力する。また、制御部２０２ｂは、木構造構築部２０４からリーフ番号を受け取り、送受信部２０７及びインターネット５を介して、受け取った機器ＩＤにより示される利用者機器へ、システムＩＤ（＝１）と受け取ったリーフ番号とを送信する。

【０２２８】さらに、制御部２０２ｂは、音楽配信用木構造テーブル２１１ｂから、所定の基準に基づいて、１個のノード鍵を選択する。ここでは、一例として、リーフからルートへの経路上に存在する全てのノードのうち、最上位のノード即ちルートに割り当てられたノード鍵を選択する。次に、制御部２０２ｂは、選択したノード鍵を、音楽コンテンツ配信装置３００へ送信する。

【０２２９】（４）公開簿生成部２０６ｂ

制御部２０２ｂが、機器ＩＤ及びシステム用機器鍵Ｓｋｄｉ$^{(i)}$　の受取りが終了したと判断する場合には、公開簿生成部２０６ｂは、システムＩＤを音楽用公開簿２２１ｂへ書き込む。次に、公開簿生成部２０６ｂは、素数＊ｐ、素数ｑを求め、積ｎ＝ｐ×ｑを演算して整数ｎを求め、整数ｎと互いに素である整数ｅを求め、整数ｎ及び整数ｅを公開鍵として音楽用公開簿２２１ｂへ書き込む。

【０２３０】次に、公開簿生成部２０６ｂは、整数Ｌ＝ＬＣＭ（ｐ－１、ｑ－１）を求める。ここで、ＬＣＭは、最小公倍数である。次に、Ｌを法とする整数ｅの逆元ｄを求める。

$$d = e^{-1} \mod L$$

ここで、整数ｎ及び整数ｄは、秘密鍵である。

【０２３１】次に、公開簿生成部２０６ｂは、階層１から階層３までの各パスについて、乱数を生成し、生成した乱数を用いて、パス情報を生成し、生成したパス情報を、階層番号及びノード番号に対応付けて、音楽配信用木構造テーブル２１１ｂへ書き込む。また、公開簿生成部２０６ｂは、インデックス情報（階層番号、パス番号）に対応付けて、生成した各パス情報を音楽用公開簿２２１ｂへ書き込む。

【０２３２】次に、公開簿生成部２０６ｂは、乱数を生成し、生成した乱数を元にしてルートに割り当てる鍵ＫｅｙＡ$^{(i)}$　を生成する。次に、生成した鍵ＫｅｙＡ$^{(i)}$　をルートに割り当てるために、（階層番号、ノード番号）＝（１、１）に対応付けて、生成した鍵ＫｅｙＡ$^{(i)}$　をノード鍵として音楽配信用木構造テーブル２１１ｂへ書き込む。

【０２３３】次に、公開簿生成部２０６ｂは、階層１から階層２への順に、さらに、各階層内の各ノードについて順に、以下に示す処理（ａ－１）～（ａ－５）を繰り返す。

（ａ－１）公開簿生成部２０６ｂは、音楽配信用木構造テーブル２１１ｂから当該ノードのノード情報を読み出し、読み出したノード情報からノード鍵を、ノード鍵ＭＫとして、抽出する

（ａ－２）新たなノード鍵＝Ｅ６（（ｄ、ｎ）、（Ｍｋ（＋）ＰＩ$_s$））
＝（Ｍｋ（＋）ＰＩ$_s$）^{d} ｍｏｄ　ｎ

を算出する。

【０２３４】ここで、ＰＩ$_s$は、当該ノードから、当該ノードの直下で左側に接続する下位ノードへのパスに対応するパス情報である。また、演算（＋）は、排他的論※

※理和を示す。

（ａ－３）新たに算出したノード鍵を、当該ノードの直下で左側に接続する下位ノードのノード情報（音楽配信用木構造テーブル２１１ｂ内の）へ書き込む。

（ａ－４）新たなノード鍵＝Ｅ６（（ｄ、ｎ）、（Ｍｋ（＋）ＰＩ$_s$））
＝（Ｍｋ（＋）ＰＩ$_s$）^{d} ｍｏｄ　ｎ

を算出する。

【０２３５】ここで、ＰＩ$_s$は、当該ノードから、当該ノードの直下で右側に接続する下位ノードへのパスに対応するパス情報である。

（ａ－５）新たに算出したノード鍵を、当該ノードの直下で右側に接続する下位ノードのノード情報（音楽配信用木構造テーブル２１１ｂ内の）へ書き込む。次に、公開簿生成部２０６ｂは、階層３内の各ノードについて順に、以下に示す処理（ｂ－１）～（ｂ－７）を繰り返す。

（ｂ－１）公開簿生成部２０６ｂは、音楽配信用木構造テーブル２１１ｂから当該ノードのノード情報を読み出し、読み出したノード情報からノード鍵を、ノード鍵ＭＫとして、抽出する。

（ｂ－２）次に、公開簿生成部２０６ｂは、当該ノードの直下で左側に接続する下位ノードのノード情報を、音楽配信用木構造テーブル２１１ｂから読み出し、読み出したノード情報からノード鍵を、ノード鍵Ｍｋ１とし

て、抽出する。
（ｂ－３）暗号化ノード情報＝Ｅ１（Ｍｋ１、Ｍｋ）を算出する。
（ｂ－４）インデックス情報とともに、算出した暗号化ノード情報を音楽用公開簿２２１ｂへ書き込む。
（ｂ－５）音楽配信用木構造テーブル２１１ｂから当該ノードの直下で右側に接続する下位ノードのノード情報を読み出し、読み出したノード情報からノード鍵を、ノード鍵Ｍｋ２として、抽出する。
（ｂ－６）暗号化ノード情報＝Ｅ１（Ｍｋ２、Ｍｋ）を算出する。
（ｂ－７）インデックス情報とともに、算出した暗号化ノード情報を音楽用公開簿２２１ｂへ書き込む。
【０２３６】次に、公開簿生成部２０６ｂは、生成した音楽用公開簿２２１ｂを、公開簿サーバ装置４００へ送信する。
（５）送受信部２０７ｂ
送受信部２０７ｂは、通信回線を介して、音楽コンテンツ配信装置３００と接続され、また、インターネット５を介して、利用者機器１１００ｂと接続されている。
【０２３７】送受信部２０７ｂは、制御部２０２と音楽コンテンツ配信装置３００との間で情報の送受信を行う。また、送受信部２０７ｂは、制御部２０２ｂと利用者機器１１００ｂとの間で情報の送受信を行う。
（６）表示部２０１ｂ及び入力部２０３ｂ
表示部２０１ｂは、制御部２０２ｂの制御の元に各種の情報を表示する。また、入力部２０３ｂは、音楽配信システム管理装置２００ｂの管理者からの情報の入力を受け付ける。
【０２３８】２．２　利用者機器１１００ｂの構成
変形例としての利用者機器１１００ｂは、利用者機器１１００と同様に、自身が記憶している機器鍵ｋｄｉ及び音楽用公開簿に基づいて、暗号化音楽コンテンツを復号して、音楽コンテンツを再生し、自身が記憶している機器鍵ｋｄｉ及びＤＶＤ用公開簿に基づいて、ＤＶＤに記録されている暗号化映画コンテンツを復号して、映画コンテンツを再生し、放送波を受信し、受信した放送波から暗号化映画コンテンツを抽出し、自身が記憶している機器鍵ｋｄｉ及び映画用公開簿に基づいて、抽出した暗号化映画コンテンツを復号して、映画コンテンツを再生する。しかしながら、利用者機器１１００ｂは、自身が記憶している機器鍵ｋｄｉ及び音楽用公開簿に基づいて、自身のために割り当てられた鍵を特定する方法において、利用者機器１１００と相違する。
【０２３９】利用者機器１１００ｂは、利用者機器１１００と同様の構成を有してる。ここでは、利用者機器１１００との相違点を中心として説明する。
（１）ノード鍵特定部１１０３
ノード鍵特定部１１０３は、情報記憶部１１０１が有するシステムＩＤテーブル１１５１から、システムＩＤに対応するリーフ番号を読み出し、機器鍵記憶部１１０２から、機器鍵ｋｄｉを読み出す。また、システムＩＤに対応する公開簿を特定する。ここでは、システムＩＤは、「１」であるので、音楽用公開簿１１６１が特定される。
【０２４０】次に、ノード鍵特定部１１０３は、システム用機器鍵$Skdi^{(0)}$＝ｈ（ｋｄｉ、システムＩＤ）を生成する。こうして、階層４のノードに割り当てられたノード鍵$Skdi^{(0)}$が求められる。次に、ノード鍵特定部１１０３は、階層３のノードに割り当てられたノード鍵を次に示すようにして、取得する。ノード鍵特定部１１０３は、リーフ番号から階層３のパス番号を求め、インデックス情報＝（３、パス番号）を設定し、音楽用公開簿１１６１から設定したインデックス情報に対応する暗号化ノード鍵を読み出し、次に、システム用機器鍵$Skdi^{(0)}$を鍵として用いて、読み出した暗号化ノード鍵を復号する。R_3＝Ｄ１（$Skdi^{(0)}$、暗号化ノード鍵）。こうして、階層３のノードに割り当てられたノード鍵R_3が求められる。
【０２４１】次に、ノード鍵特定部１１０３は、階層２～１のノードに割り当てられたノード鍵を次に示すようにして、取得する。ノード鍵特定部１１０３は、音楽用公開簿１１６１から公開鍵ｅ、ｎを読み出し、R_2＝Ｄ６（（ｅ、ｎ）、R_3）＝（R_3）＊ｍｏｄ　ｎ　を算出する。次に、ノード鍵特定部１１０３は、リーフ番号から階層２のパス番号を求め、インデックス情報＝（２、パス番号）を設定し、音楽用公開簿１１６１から設定したインデックス情報に対応するパス情報を、パス情報ＰＩとして、読み出し、R_2＝R_2　（＋）ＰＩを算出する。こうして、階層２のノードに割り当てられたノード鍵R_2が求められる。
【０２４２】次に、ノード鍵特定部１１０３は、R_1＝Ｄ６（（ｅ、ｎ）、R_2）＝（R_2）＊ｍｏｄ　ｎ　を算出する。次に、ノード鍵特定部１１０３は、リーフ番号から階層１のパス番号を求め、インデックス情報＝（１、パス番号）を設定し、音楽用公開簿１１６１から設定したインデックス情報に対応するパス情報を、パス情報ＰＩとして、読み出し、R_1＝R_1　（＋）ＰＩを算出する。こうして、階層２のノードに割り当てられたノード鍵R_2が求められる。
【０２４３】次に、ノード鍵特定部１１０３は、$Skdi^{(0)}$、R_3、R_2、R_1のうちから１個のノード鍵を決定する。
２．３　音楽配信システム管理装置２００ｂの動作
音楽配信システム管理装置２００ｂの動作について、図４７～図５１に示すフローチャートを用いて説明する。
【０２４４】木構造構築部２０４ｂは、音楽配信用木構造テーブル２１１ｂを生成して情報記憶部２０８ｂへ書き込む（ステップＳ４３１）。次に、制御部２０２ｂは、鍵管理装置１００から送受信部２０７ｂを介して、

機器ＩＤ及びシステム用機器鍵Ｓｋｄｉ$^{(0)}$　を受け取り、受け取った機器ＩＤ及びシステム用機器鍵Ｓｋｄｉ$^{(0)}$　を木構造構築部２０４ｂへ出力する（ステップＳ４３２）。次に、木構造構築部２０４ｂは、音楽配信用木構造テーブル２１１ｂにおいて、受け取ったシステム用機器鍵Ｓｋｄｉ$^{(0)}$　が１個のリーフに対応するように、機器ＩＤ及びシステム用機器鍵Ｓｋｄｉ$^{(0)}$　を音楽配信用木構造テーブル２１１ｂに書き込む（ステップＳ４３３）。次に、制御部２０２ｂは、送受信部２０７及びインターネット５を介して、受け取った機器ＩＤにより示される利用者機器へ、システムＩＤ（＝１）とリーフ番号とを送信する（ステップＳ４３４）。

【０２４５】次に、制御部２０２ｂは、機器ＩＤ及びシステム用機器鍵Ｓｋｄｉ$^{(0)}$　の受取りが終了したか否かを判断し、終了していないと判断する場合には（ステップＳ４３６）、ステップＳ４３２へ戻って処理を繰り返す。制御部２０２ｂが、機器ＩＤ及びシステム用機器鍵Ｓｋｄｉ$^{(0)}$　の受取りが終了したと判断する場合には（ステップＳ４３６）、さらに、公開簿生成部２０６ｂは、システムＩＤを音楽用公開簿２２１ｂへ書き込む（ステップＳ４３７）。

【０２４６】次に、公開簿生成部２０６ｂは、素数ｐ、素数ｑを求め（ステップＳ４３８）、積ｎ＝ｐ×ｑを演算して整数ｎを求め（ステップＳ４３９）、整数ｎと互いに素である整数ｅを求め（ステップＳ４４０）、整数ｎ及び整数ｅを公開鍵として音楽用公開簿２２１ｂへ書き込む（ステップＳ４４１）。次に、公開簿生成部２０６ｂは、整数Ｌ＝ＬＣＭ（ｐ－１、ｑ－１）を求める。ここで、ＬＣＭは、最小公倍数である（ステップＳ４４２）。次に、Ｌを法とする整数ｅの逆元ｄを求める。ｄ＝ｅ$^{-1}$　ｍｏｄ　Ｌ（ステップＳ４４３）。

【０２４７】次に、公開簿生成部２０６ｂは、階層１から階層３までの各パスについて、パス情報を生成し、生成したパス情報を、階層番号及びノード番号に対応付けて、音楽配信用木構造テーブル２１１ｂへ書き込み（ステップＳ４４４）、インデックス情報（階層番号、パス番号）に対応付けて、生成した各パス情報を音楽用公開簿２２１ｂへ書き込む（ステップＳ４４５）。

【０２４８】次に、公開簿生成部２０６ｂは、乱数を生成し、生成した乱数を元にしてルートに割り当てる鍵ＫｅｙＡ$^{(0)}$　をルートに割り当てるために、（階層番号、ノード番号）＝（１、１）に対応付けて、鍵ＫｅｙＡ$^{(0)}$　をノード鍵として音楽配信用木構造テーブル２１１ｂへ書き込む（ステップＳ４４６）。

【０２４９】次に、公開簿生成部２０６ｂは、ステップＳ４４７からステップＳ４５６において、階層１から階層２まで（階層の番号ｍ＝１、２）、順に、以下に示すステップＳ４４８～ステップＳ４５５を繰り返す。次に、公開簿生成部２０６ｂは、ステップＳ４４８からステップＳ４５５において、階層番号ｍにより示される階層内の各ノードについて順に、以下に示すステップＳ４４９～ステップＳ４５４を繰り返す。

【０２５０】公開簿生成部２０６ｂは、音楽配信用木構造テーブル２１１ｂから当該ノードのノード情報を読み出し（ステップＳ４４９）、読み出したノード情報からノード鍵を、ノード鍵Ｍｋとして、抽出する（ステップＳ４５０）。次に、新たなノード鍵＝Ｅ６（（ｄ、ｎ）、（Ｍｋ（＋）ＰＩ。））＝（Ｍｋ（＋）ＰＩ。）^{4}ｍｏｄ　ｎ　を算出し（ステップＳ４５１）、新たに算出したノード鍵を、当該ノードの直下で左側に接続する下位ノードのノード情報（音楽配信用木構造テーブル２１１ｂ内の）へ書き込む（ステップＳ４５２）。さらに、新たなノード鍵＝Ｅ６（（ｄ、ｎ）、（Ｍｋ（＋）ＰＩ。））＝（Ｍｋ（＋）ＰＩ。）^{4}ｍｏｄｎ　を算出し（ステップＳ４５３）、新たに算出したノード鍵を、当該ノードの直下で右側に接続する下位ノードのノード情報（音楽配信用木構造テーブル２１１ｂ内の）へ書き込む（ステップＳ４５４）。

【０２５１】次に、公開簿生成部２０６ｂは、ステップＳ４５７からステップＳ４６８において、階層３内の各ノードについて順に、以下に示すステップＳ４５８～ステップＳ４６７を繰り返す。公開簿生成部２０６ｂは、音楽配信用木構造テーブル２１１ｂから当該ノードのノード情報を読み出し（ステップＳ４５８）、読み出したノード情報からノード鍵を、ノード鍵Ｍｋとして、抽出する（ステップＳ４５９）。

【０２５２】次に、公開簿生成部２０６ｂは、当該ノードの直下で左側に接続する下位ノードのノード情報を、音楽配信用木構造テーブル２１１ｂから読み出し（ステップＳ４６０）、読み出したノード情報からノード鍵を、ノード鍵Ｍｋ１として、抽出し（ステップＳ４６１）、暗号化ノード情報＝Ｅ１（Ｍｋ１、Ｍｋ）を算出し（ステップＳ４６２）、インデックス情報とともに、算出した暗号化ノード情報を音楽用公開簿２２１ｂへ書き込む（ステップＳ４６３）。

【０２５３】次に、音楽配信用木構造テーブル２１１ｂから当該ノードの直下で右側に接続する下位ノードのノード情報を読み出し（ステップＳ４６４）、読み出したノード情報からノード鍵を、ノード鍵Ｍｋ２として、抽出し（ステップＳ４６５）、暗号化ノード情報＝Ｅ１（Ｍｋ２、Ｍｋ）を算出し（ステップＳ４６６）、インデックス情報とともに、算出した暗号化ノード情報を音楽用公開簿２２１ｂへ書き込む（ステップＳ４６７）。

【０２５４】次に、公開簿生成部２０６ｂは、生成した音楽用公開簿２２１ｂを、公開簿サーバ装置４００へ送信し（ステップＳ４６９）、制御部２０２ｂは、音楽配信用木構造テーブル２１１ｂから、１個のノード鍵を選択し（ステップＳ４７０）、選択したノード鍵を、音楽コンテンツ配信装置３００へ送信する（ステップＳ４７

1）。

【０２５５】２．４　利用者機器１１００ｂの動作

利用者機器１１００ｂの動作のうち、ノード鍵特定部１１０３ｂによるノード鍵の特定（１）の動作について、図５２～図５３に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図３４のフローチャートのステップＳ３０７の詳細である。

【０２５６】ノード鍵特定部１１０３ｂは、情報記憶部１１０１ｂが有するシステムＩＤテーブル１１５１から、システムＩＤに対応するリーフ番号を読み出し（ステップＳ４９１）、機器鍵記憶部１１０２ｂから、機器鍵ｋｄｉを読み出し（ステップＳ４９２）、システムＩＤに対応する公開簿を特定する。ここでは、システムＩＤは、「１」であるので、音楽用公開簿１１６１が特定される（ステップＳ４９３）。

【０２５７】次に、ノード鍵特定部１１０３ｂは、システム用機器鍵$Skdi^{(0)}$＝ｈ（ｋｄｉ、システムＩＤ）を生成し（ステップＳ４９４）、リーフ番号から階層３のパス番号を求め（ステップＳ４９５）、インデックス情報＝（３、パス番号）を設定し（ステップＳ４９６）、音楽用公開簿１１６１から設定したインデックス情報に対応する暗号化ノード鍵を読み出し（ステップＳ４９７）、次に、システム用機器鍵$Skdi^{(0)}$を鍵として用いて、読み出した暗号化ノード鍵を復号する。R_3＝Ｄ１（$Skdi^{(0)}$、暗号化ノード鍵）（ステップＳ４９８）。

【０２５８】次に、ノード鍵特定部１１０３ｂは、音楽用公開簿１１６１から公開鍵ｅ、ｎを読み出し（ステップＳ４９９）、R_2＝Ｄ６（（ｅ、ｎ）、R_3）＝（R_3）*ｍｏｄ　ｎ　を算出する（ステップＳ５００）。次に、ノード鍵特定部１１０３ｂは、リーフ番号から階層２のパス番号を求め（ステップＳ５０１）、インデックス情報＝（２、パス番号）を設定し（ステップＳ５０２）、音楽用公開簿１１６１から設定したインデックス情報に対応するパス情報を、パス情報ＰＩとして、読み出し（ステップＳ５０３）、R_2＝R_2（＋）ＰＩを算出し（ステップＳ５０４）、R_1＝Ｄ６（（ｅ、ｎ）、R_1）＝（R_2）*ｍｏｄ　ｎ　を算出する（ステップＳ５０５）。

【０２５９】次に、ノード鍵特定部１１０３ｂは、リーフ番号から階層１のパス番号を求め（ステップＳ５０６）、インデックス情報＝（１、パス番号）を設定し（ステップＳ５０７）、音楽用公開簿１１６１から設定したインデックス情報に対応するパス情報を、パス情報ＰＩとして、読み出し（ステップＳ５０８）、R_1＝R_1（＋）ＰＩを算出する（ステップＳ５０９）。

【０２６０】次に、ノード鍵特定部１１０３ｂは、$Skdi^{(0)}$、R_3、R_2、R_1のうちから１個のノード鍵を決定する（ステップＳ５１０）。

３．まとめ

３．１　本発明の概要

以上説明したように、本発明は、１個の利用者機器が、異なる複数のコンテンツ配信システムに接続され、各コンテンツ配信システムからコンテンツの配信サービスの提供を受ける際に、それぞれのコンテンツ配信システムにおいて、柔軟でかつそれぞれ独自の木構造を用いてグループ鍵の管理を行うことができる暗号化伝送システムに関する。

【０２６１】各利用者機器は、木構造のリーフに対応した機器鍵を保持しており、機器鍵とシステム毎に公開されている公開簿を用いて、リーフから順次上位に木構造を再構成し、各利用者機器に対応するノード鍵を求め、求めたノード鍵に基づいて、暗号化コンテンツを復号する。公開簿は、それぞれのシステムが提供するＷｅｂサーバ、ＤＶＤなどのパッケージメディア、デジタル放送により各利用者機器に対して公開される。

【０２６２】鍵管理機関により管理運営される鍵管理装置は、機器鍵を安全に保存するとともに、機器鍵を対応する利用者機器に配布する。また、コンテンツ供給システムのシステム管理者に対し、システム用機器鍵を配布する。ここで、システム用機器鍵は、機器鍵を当該コンテンツ供給システム用に変換した鍵である。コンテンツ供給システムのシステム管理装置は、システム用機器鍵を用いて、木構造を構築し公開簿を生成し、これを管理する。また、コンテンツ供給システムのコンテンツ供給者に対して、グループ鍵を暗号化するために必要となる各ノード鍵を指定する。

【０２６３】コンテンツ供給システムのコンテンツ供給装置は、各利用者機器に対し、コンテンツ供給システム固有のコンテンツサービスを提供する。コンテンツ供給装置は、コンテンツに対応してグループ鍵を生成し、グループ鍵をシステム管理装置から受け取ったノード鍵を用いて暗号化して、暗号化鍵情報（グループ鍵を特定の利用者機器で求めるための鍵情報）を生成し、グループ鍵を用いて暗号化されたコンテンツとともに、各利用者機器に配布する。

【０２６４】各利用者機器は、予め鍵管理装置から配布された固定で個別の機器鍵を有し、機器鍵を用いて、各利用者機器が加入しているコンテンツ供給システムのためのシステム用機器鍵を生成し、コンテンツ供給装置から供給される暗号化鍵情報及び暗号化コンテンツを受信する。ここで、各利用者機器に関して、次のように仮定する。

【０２６５】（ａ）各利用者機器が有している機器鍵は変更されない。機器鍵は、例えば、製造時に埋め込まれるものとする。

（ｂ）各利用者機器は、異なる複数のコンテンツ供給システムに加入可能であり、それぞれのコンテンツ供給システムにより提供されるコンテンツサービスを受けることができる。

【０２６６】（ｃ）各利用者機器は、デジタル放送、ホームページ、パッケージメディアなどにより、公開される開簿にアクセス可能である。

３．２　運用手順の例

次に、運用手順の例について説明する。

＜１＞利用者機器の製造時

ここで、利用者機器のＩＤをｉとする。

【０２６７】鍵管理装置は、対応する利用者機器ｉの機器鍵ｋｄｉを生成し、安全に保管すると共に、製造業者を介して、利用者機器ｉの製造時に、機器鍵ｋｄｉを利用者機器ｉに埋め込む。

＜２＞コンテンツ供給システムの立上げ時

コンテンツ供給システムのＩＤをＩＤ１とする。

【０２６８】（１）鍵管理装置は、コンテンツ供給システムのＩＤを用いて、システム用の機器ｉの鍵ｈ（ｋｄｉ、ＩＤ１）を求める。ここでｈは、公開の一方向性関数とする。システム用の機器鍵の生成に一方向性関数を用いることにより、コンテンツ供給システムのシステム管理者は、システム用の機器鍵から機器の鍵自身ｋｄｉを求めることもできないし、また、他のコンテンツ供給システム用の機器鍵を求めることもできない。

【０２６９】（２）鍵管理装置は、コンテンツ供給システムに加入する利用者機器のシステム用機器鍵をコンテンツ供給システムのシステム管理者が管理、遡営するシステム管理装置へ秘密に渡す。

（３）システム管理装置は、任意にグループ鍵を管理するための木構造を構築し、さらに、システム用機器鍵を用いて公開簿を生成する。

【０２７０】（４）システム管理装置は、生成した公開簿を、例えば、デジタル放送、Ｗｅｂサーバや、パッケージメディアを用いて、利用者機器に対して公開する。

＜３＞コンテンツ配布時

（１）システム管理装置は、コンテンツを渡す相手の利用者機器を管理し、コンテンツを暗号化するために使用する木構造のノード鍵を選ぶ。システム管理装置は、選んだノード鍵（デバイス鍵と称することもある）を、コンテンツ供給装置へ配布する。コンテンツは、選ばれたノード鍵（デバイス鍵）に基づいて、暗号化される。なお、ここでは、システム管理装置が、コンテンツを暗号化する際に基づくノード鍵の選択を行うものとしているが、コンテンツ供給装置が行うとしてもよい。

【０２７１】（２）コンテンツ供給装置は、任意のグループ鍵を生成し、生成したグループ鍵をシステム管理装置により指定されたノード鍵を用いて暗号化し、その結果を暗号化鍵情報とし、暗号化鍵情報と、グループ鍵を用いて暗号化されたコンテンツとともに、例えば、インターネット、ＤＶＤなどのパッケージメディアや、放送メディアを用いて利用者機器に供給する。

【０２７２】（３）利用者機器は、自身の機器鍵ｋｄｉとコンテンツ供給システムのＩＤを用いて、コンテンツ供給システム用の機器鍵ｈ（ｋｄｉ、ＩＤ１）を求める。

（４）利用者機器は、システム用の機器鍵と公開簿を用いてコンテンツ供給システムの木構造における自身のノード鍵を順次求める。

（５）利用者機器は、コンテンツ供給装置から供給された暗号化鍵情報から自身に対応する暗号文を選び、ノード鍵を用いて復号してグループ鍵を求め、さらにグループ鍵を用いてコンテンツを求める。

【０２７３】ここまでにおいて、１個のコンテンツ供給システムの場合のみについて説明してきたが、さらに、別のコンテンツ供給システムシステムが追加される場合も、前記コンテンツ供給システムの立上げおよび運用と同様に行えばよい。このとき、利用者機器ｉは、公開の一方向性関数とシステムのＩＤを用いて、内部で新たなコンテンツ供給システム用の機器鍵を生成するだけでよく、例えば、ＩＣカードなどの別途の方法を用いて利用者機器に秘密鍵等を追加する必要はない。

【０２７４】次に、上記の公開簿の生成方法、及び利用者機器において機器鍵からコンテンツを復号するため必要なノード鍵の求め方について、４つの具体例を述べる。なお、例として、コンテンツ供給システムが、３階層の木構造分割方法に対応した公開簿を生成する場合について述べる。各利用者機器ｉは、機器鍵のみを保持し、機器鍵より一方向性関数を用いてシステム用機器鍵$Skd_i^{(0)}$（＝ｈ（ｋｄｉ、ＩＤ１））を求める。また各利用者機器ｉは、公開簿を用いて木構造における対応するノード鍵を求める。また、ｈ、ｇを公開の一方向性関数とする。

【０２７５】＜４＞具体例１＝共通鍵暗号を利用した方法

具体例１は、音楽配信システム２において説明したものに対応する。

（１）システム管理装置による木構造の決定

システム管理装置は、コンテンツ供給システムに加入する利用者機器のシステム用機器鍵$Skd_1^{(0)}$～$Skd_8^{(0)}$を木構造のリーフに割り当て、図６に示す木構造の各ノード鍵を任意に決める。

【０２７６】（２）システム管理装置による公開簿の生成

システム管理装置は、木構造の各パスに対応した暗号文を生成する。例えば、利用者機器１のリーフから$KeyD^{(0)}$が割り当てられたノードへのパスに対応して、コンテンツ供給システム用の機器鍵$Skd_1^{(0)}$を鍵として用いて、$KeyD^{(0)}$を暗号化して、暗号文$E1(Skd_1^{(0)}, KeyD^{(0)})$を求める。なお、暗号化アルゴリズムＥＩは、例えば、ＤＥＳやＡＥＳなどの共通鍵暗号とし、これに対応する復号アルゴリズムＤＩは公開されているものとする。

【０２７７】また、機器２のリーフから$KeyD^{(0)}$が

割り当てられたノードへのパスに対応しては、Ｅ１（Ｓｋｄ２$^{(2)}$、ＫｅｙＤ$^{(2)}$）を求める。以下同様に求めて、これらを図８に示す公開簿に公開する。なお、公開簿には暗号文とともに、その暗号文がどのパスに対応した暗号文なのかを示すインデックス情報を載せる。インデックス情報の例としては、木構造の階層番号とその階層における左からの番号とを用いることができる。暗号文Ｅ１（ｋｄ１$^{(2)}$、ＫｅｙＤ$^{(2)}$）のインデックス情報としては、例えば、上位から３層目の最も左のパスであることより、（３，１）を付加する。以下同様である。

【０２７８】（３）各利用者機器によるノード鍵の算出
各利用者機器は、システム用の機器鍵から、上記公開簿を用いて順次木構造を上にたどり、ノード鍵を求める。例えば、機器ＩＤが「１００１」である利用者機器１は、まず、自身の機器鍵ｋｄ１とシステム１のＩＤ番号を一方向性関数ｈの入力として、コンテンツ供給システム用の機器鍵Ｓｋｄ１$^{(2)}$　を求める。そして、公開簿からＥ１（Ｓｋｄ１$^{(2)}$、ＫｅｙＤ$^{(2)}$）を取り出して、これを復号して、１つ上の層のノード鍵ＫｅｙＤ$^{(2)}$　を求める。さらに、Ｅ１（ＫｅｙＤ$^{(2)}$，ＫｅｙＢ$^{(2)}$）を復号して、さらに、上位層のノード鍵ＫｅｙＢ$^{(2)}$　を求める。最後に、Ｅ１（ＫｅｙＢ$^{(2)}$、ＫｅｙＡ$^{(2)}$）を復号して、ルートのＫｅｙＡ$^{(2)}$　を求める。なお、公開簿から所望の暗号文を取り出すには、予め機器内に埋め込まれている木構造における自身の位置情報とインデックス情報とを用いる。なお、利用者機器が上記獲得したノード鍵のうちどれを用いて、コンテンツ供給者から供給されたコンテンツを復号するのかについては、従来どおりコンテンツに付随して供給される暗号化鍵情報を用いる。

【０２７９】＜５＞具体例２＝一方向性関数を利用した方法
具体例２は、ＤＶＤ供給システム３において説明したものに対応する。具体例２は、具体例１における各ノードの左パスに一方向性関数を用いることにより、公開簿のデータ容量を削減している。

（１）システム管理装置による木構造の決定
システム管理装置は、コンテンツ供給システムに加入する利用者機器のシステム用機器鍵Ｓｋｄ１$^{(2)}$　～Ｓｋｄ８$^{(2)}$　を、図１３に示す木構造のリーフに割り当てる。

【０２８０】（２）システム管理装置による公開簿の生成
システム管理装置は、一方向性関数ｇを用いて、ｇ（Ｓｋｄ１$^{(2)}$）、ｇ（Ｓｋｄ３$^{(2)}$）、ｇ（Ｓｋｄ５$^{(2)}$）、ｇ（Ｓｋｄ７$^{(2)}$）をそれぞれ求めて、リーフの１つ上の層のノード鍵ＫｅｙＤ$^{(2)}$、ＫｅｙＥ$^{(2)}$、ＫｅｙＦ$^{(2)}$、ＫｅｙＧ$^{(2)}$　とする。

【０２８１】システム管理装置者は、公開簿に、Ｅ４（Ｓｋｄ２$^{(2)}$、ＫｅｙＤ$^{(2)}$）、Ｅ４（Ｓｋｄ４$^{(2)}$、ＫｅｙＥ$^{(2)}$）、Ｅ４（Ｓｋｄ６$^{(2)}$、ＫｅｙＦ$^{(2)}$）、Ｅ４（Ｓｋｄ８$^{(2)}$、ＫｅｙＧ$^{(2)}$）を登録する。なお、ここで例えばＥ４（Ｓｋｄ２$^{(2)}$、ＫｅｙＤ$^{(2)}$）は、Ｓｋｄ２$^{(2)}$　を鍵としてノード鍵ＫｅｙＤ$^{(2)}$　を共通鍵暗号化して生成した暗号文である。

【０２８２】同様に、順次木構造の左パスは一方向性関数ｇでその層の鍵を求め、右パス用の暗号文を公開簿に登録する。結果として図１４に示す公開簿を生成して、公開する。

（３）各利用者機器によるノード鍵の算出
リーフに対応した機器鍵を保持する各利用者機器は、まず一方向性関数ｈを用いてシステム用機器鍵を求める。次に、木構造における左パスを上位層にたどるときは一方向性関数ｇを用い（図１３において、実線で表す）、右パスをたどるときは公開簿の対応する暗号文を復号して（図１３において、二重線で表す）、順次ルートに至るまでのノード鍵を求める。

【０２８３】例えば、機器ＩＤが「１００３」である利用者機器３は、まず一方向性関数ｇを用いてＫｅｙＥ$^{(2)}$　を求め、次に公開簿から　Ｅ４（ＫｅｙＥ$^{(2)}$、ＫｅｙＢ$^{(2)}$）を復号してＫｅｙＢ$^{(2)}$　を求める。さらに、ｇを用いてＫｅｙＡ$^{(2)}$　を求める。なお、この例では左パスを一方向性関数を用いてたどるとしたが、層ごとに一方向性関数を用いるパスを変えてもよい。また、ここでは同じ一方向性関数を用いているが、層ごとに異なる関数を用いても良い。一方向性関数を用いてたどるのか、公開簿を用いてたどるのか、あるいはどの一方向性関数を用いるのかの判断は、具体例１と同様に木構造におけるの当該機器の位置と公開簿内の暗号文に付加するインデックス情報を用いればよい。

【０２８４】＜６＞具体例３＝秘密分散のテクニックを利用した方法
具体例３は、映画放送システム４において説明したものに対応する。具体例３は、下位ノード鍵から共通の曲線（次数が１の場合は直線）を求めて、曲線から一意に決定される点を上位のノード鍵とする。この方法は秘密分散と同様のテクニックである。なお、以下の曲線は、（以下特に説明はしないが）ある体上で求められるものとする。

【０２８５】（１）システム管理装置による木構造の決定
システム管理装置は、システムに加入する利用者機器のシステム用機器鍵Ｓｋｄ１$^{(2)}$　～Ｓｋｄ８$^{(2)}$　を、図１６に示す木構造のリーフに割り当てる。木構造のリーフにあたる機器鍵を、（ｘ，ｙ）平面上の点とする。

（２）システム管理装置による木構造と公開簿の生成
システム管理装置は、Ｓｋｄ１$^{(2)}$　及びＳｋｄ２$^{(2)}$　を通る直線を求め、直線上の点をｓ１として公開する。ｓ１のｘ座標を予め決めておき、これをＡ公開簿に載せて（ここではｘ$_0$　とする）、ｓ１のｙ座標ｓ１$_{y0}$　だけを

公開簿に登録する。

【０２８６】直線からある決められた手順で同じ直線上のＫｅｙＤ(0)を求める。なお、直線を求めた人だけがＫｅｙＤ(0)を求めることができるようにする。そのためには、例えば、この手順の中に一方向性関数ｇを含めればよい。例えば図１８に示す例では、直線の切片ｙをｘ一方向性関数で変換し、この値ｇ（ｙ）をｘ座標とする直線上の点をＫｅｙＤ(2)としている。一方向性関数を用いることにより、利用者機器１と利用者機器２以外の利用者機器は、ＫｅｙＤ(0)のｘ座標を求めることができない。

【０２８７】システム管理装置は、ＫｅｙＤ(0)、ＫｅｙＥ(3)ω　として公開し、ＫｅｙＢ(3)を求める。利用者機器１～利用者機器４は、ＫｅｙＤ(2)及びＫｅｙＥ(0)を通る直線を求めることができるが、上記の理由により、利用者機器３と利用者機器４は、この直線より、ＫｅｙＤ(3)を求めることが困難である。

【０２８８】以下同様に、順次２つのノード鍵からその共通の上位ノード鍵と、公開簿への登録値を順次求める。公開簿への登録値を図２０に示す。ここでの各登録値は、Ｓｋｄ１(3)、Ｓｋｄ２(3)と公開値ｓ１および上位のノード鍵ＫｅｙＤの関係を、図１９のように標記したときの、図１６に示した点ｓ１～ｓ７のｙ座標である。

【０２８９】（３）各利用者機器によるノード鍵の算出
各利用者機器は、自身の機器鍵と公開簿に登録されている値（双方とも（ｘ，ｙ）平面上の点）を通る直線を求め、順次上位の階層のノード鍵を求める。例えば、利用者機器１はまずシステム用機器鍵を求め、これとｓ１を通る直線よりＫｅｙＤ(0)を求める。次にＫｅｙＤ(0)とｓ５を通る直線よりＫｅｙＢ(0)を求め、同様に順次、ＫｅｙＡ(0)を求める。

【０２９０】なお、この例では２進木の場合を述べたが、例えば３進木の場合はある親ノードから派生する３つのノードのノード鍵３点を通る２次曲線を求め、この上の任意の２点を公開簿に掲載する。利用者機器は自身が保持するノード鍵１点と、公開簿の２点より上記２次曲線を求め、１つ上のノード鍵を求める。

＜７＞具体例４＝ＲＳＡを利用した方法
具体例４は、音楽配信システム２の変形例として説明したものに対応する。

【０２９１】（１）システム管理装置による木構造の決定
システム管理装置は、システムに加入する機器のシステム用機器鍵Ｓｋｄ１(c)～Ｓｋｄ８(0)を、図４４に示す木構造のリーフに割り当てる。

（２）システム管理装置による木構造と公開簿の生成
ＲＳＡ暗号と同様に、素数ｐ、ｑを求めその積ｎ＝ｐ×ｑを公開する。ｎと互いに素なｅを求めて公開すると共に、Ｌ（＝ＬＣＭ（ｐ－１，ｑ－１）：ＬＣＭは最小公倍数）を法としたｅの逆元ｄ（＝e^{-1}　ｍｏｄ　Ｌ：ｄは、秘密鍵）を求める。システム管理装置は、例えば図４４に示すように各パスに対応したパス情報を決定し公開する。任意にルートの鍵ＫｅｙＡ(0)を求め、ＫｅｙＡ(0)と（左のパスの）パス情報ｐ１の排他的論理和を求めて、これを秘密鍵ｄを用いて暗号化した結果をＫｅｙＢ(0)とする。また、ＫｅｙＡ(0)と（右のパスの）パス情報ｐ２の排他的論理和を求め、これをｄで暗号化した結果をＫｅｙＣ(0)とする。以下同様にリーフの１つ上の層のノード鍵まで求める。以上で生成した公開簿を図４６に示す。

【０２９２】最後の１層については、具体例１、具体例２、又は具体例３の方法を用いて、対応する公開簿を生成する。

（３）各利用者機器によるノード鍵の算出
利用者機器は、具体例１、具体例２、又は具体例３の方法を用いて１つ上の層のノード鍵を求める。例えば、利用者機器１は、ＫｅｙＤ(0)を求める。次に、ＫｅｙＤ(0)を公開鍵ｅで復号し、その結果とパス情報ｐ３の排他的論理和を求めて上位層のノード鍵ＫｅｙＢ(0)を求める。さらに、ＫｅｙＢ(1)を公開鍵ｅで復号し、その結果とパス情報ｐ１との排他的論理和を求めてルートの鍵ＫｅｙＡ(0)を求める。

【０２９３】４．その他の変形例
なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

（１）暗号化データ配信システム１において、３個のコンテンツ供給システムが含まれているとしているが、さらに多くのコンテンツ供給システムを含むとしてもよい。

【０２９４】また、１個のコンテンツ供給システム内において、１個の木構造を有し、前記１個の木構造を用いて、鍵を管理しているが、１個のコンテンツ供給システム内において、複数の木構造を有し、前記複数の木構造を用いて、鍵を管理するとしてもよい。このとき、複数の公開簿が公開される。また、１個のコンテンツ供給システム内において、複数のコンテンツ供給装置を含むとしてもよい。

【０２９５】また、例えば、音楽配信システム２において、音楽配信システム管理装置２００と音楽コンテンツ配信装置３００とは、一体の装置であるとしてもよい。また、暗号化データ配信システム１において、３個のコンテンツ供給システムが含まれ、３個のコンテンツ供給システムにおいて、それぞれ異なる公開簿の生成及び鍵管理方法を採用しているが、これらのうち、２個のコンテンツ供給システムにおいて、同一の公開簿生成方法及び同一の鍵管理方法を採用するとしてもよい。

【０２９６】（２）以上述べた具体例１～具体例４で求めた各利用者機器におけるノード鍵は、使用した後、利用者機器やシステムに依存して運用、管理することができる。例えば、頻繁にそのシステムを利用する場合や、多くのメモリを備えた利用者機器であれば、そのまま保管しておけば、上記計算しなくてもすぐに利用することができる。

【０２９７】また、あまりそのシステムを利用しない場合や、小さなメモリしかない利用者機器では、そのたびに必要なノード鍵を計算したほうが効率的である。リーフから途中の層までのノード鍵をメモリに保管し、それから上位は計算で求める等、柔軟に運用することもできる。また、もし、利用者機器が不当に搾取されてしまった場合を考慮すると、ノード鍵を機器の中に保管していないほうが良いこともある。システム管理装置は、ある利用者機器が搾取されたことが判明したら、その利用者機器がより上位層のノード鍵を求めるための情報を公開簿から消してしまう。このことにより、搾取された利用者機器をグループからはずすことができる。公開簿を先にコピーされていたり、搾取してすぐにノード鍵を求めて保管しておくなども可能なので、ある利用者機器をグループからはずす方法としては完全ではないが、簡易に対応できるため運用上は有効である。この場合には、計算したノード鍵による処理が終了したら削除するよう、システム管理装置から利用者機器に指示する。

【０２９８】（３）また、上記の具体例１～具体例４の各方法を組み合わせてもかまわない。例えば、木構造のリーフから１つ上の層のノード鍵を求めるためには、具体例１を用いて、それから上位の層のノード鍵を求めるためには具体例４の方法を用いるなどである。

（４）また、ここでの公開簿を利用者機器に供給する場合は、例えばシステムが管理するＷｅｂページやＤＶＤなどのパッケージメディアを用いればよい。またＷｅｂページやパッケージメディアはシステムに１つではなく、複数に分けて管理して配布してもよい。また、当該利用者機器に関連する部分的な公開情報だけを選んで、インターネットなどを用いて送付してもよい。

【０２９９】（５）また、ここで述べた木構造構築方法は、次の目的のためにも利用することができる。

（ａ）ある時間ごとにノード鍵を変更する。

（ｂ）多くの利用者機器がグループから排除され、小さな木に分割されて暗号化鍵情報の情報量が多くなったときに、残っている利用者機器で木を整える。この後、暗号化鍵情報量を初期状態に戻すことが出来る。

【０３００】（６）システム管理者とコンテンツ供給者を分けているが、同一機関であってもよい。つまり、システム管理装置とコンテンツ供給装置とが同一の装置であってもよい。

（７）各利用者機器は、機器鍵から対応するシステム用機器鍵を、コンテンツ供給システムの運用開始時に都度作成するとしているが、コンテンツ供給システムから供給されるものであっても良いし、機器作成時にシステム用機器鍵がすでに決っているコンテンツ供給システムであれば予め利用者機器に埋め込んでおいてもよい。

【０３０１】（８）コンテンツを任意に生成したグループ鍵で暗号化し、さらに、グループ鍵をあるノード鍵で暗号化する場合で説明したが、より一般的に単なるデータをあるノード鍵で暗号化するとしてもよい。

（９）コンテンツ供給システムを例にして、コンテンツ供給システムごとにシステム管理者とコンテンツ配信者が存在する場合で説明したが、より一般的に単なる暗号化装置としてもよい。

【０３０２】（１０）上記に説明した複数の木構造は、それぞれ、４階層から構成される２分木であるとしているが、これには限定されない。前記複数の木構造は、さらに多くの階層を有してるとしてもよいし、また、前記複数の木構造は、それぞれ異なる階層数の木構造からなるとしてもよい。また、前記複数の木構造は、３分木、４分木などであるとしてもよい。前記複数の木構造は、一般的に、ｎ分木であるとしてもよい。ここで、ｎは、２以上の整数である。

【０３０３】（１１）上記に説明した各コンテンツ供給システムは、音楽及び映画のコンテンツを供給するとしているが、他のコンテンツを供給するとしてもよい。また、上記に説明した各コンテンツ供給システムは、インターネット、ＤＶＤなどのパケージメディア、放送メディアを介して、コンテンツを供給するとしているが、他のメディアを介して、コンテンツを供給するとしてもよい。

【０３０４】（１２）上記に説明した鍵管理装置は、利用者機器に固有の機器鍵を生成するとしているが、これには限定されない。例えば、利用者機器が自身で固有の機器鍵を生成し、生成した機器鍵を鍵管理装置に秘密に登録するようにしてもよい。

（１３）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

【０３０５】また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＢＤ（Ｂｌｕ－ｒａｙ Ｄｉｓｃ）、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【０３０６】また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は

有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

【０３０７】また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。（１４）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【０３０８】

【発明の効果】今後、１個の利用者機器が、複数のコンテンツ供給システムに接続されることが予測できる。例えば、ＳＴＢ（セットトップボックス）は、家庭内の機器のゲートウェイマシンの役割を担い、パッケージメディア、放送、インターネットなどに接続されると予測される。このため、ＳＴＢは、複数のコンテンツ供給システムに対応する必要がある。一方で、前記複数のコンテンツ供給システムにおいて、それぞれ用いられる暗号化のための鍵の管理方法が１つに統一されることは困難であると思われる。

【０３０９】ある利用者機器が、複数システムの木構造鍵管理に対応するために、次の２つの方法が考えられる。

（第１の方法）すべてのコンテンツ供給システムが、共通の１つの木構造を利用する。

（第２の方法）１個の利用者機器が、コンテンツ供給システムにおいて個別に定められたそれぞれ独立した木構造を備える。つまり、利用者機器は、複数の木構造のリーフからルートに至るノード鍵をすべて保持する。

【０３１０】上記２つの方法には、以下の課題がある。

（ａ）柔軟性の欠如（第１及び第２の方法に共通の課題）

第２の方法では、利用者機器の製造時に、利用者機器で使用するコンテンツ供給システムをすべて決め、あらかじめ対応するノード鍵を格納しておく必要がある。このため、利用者機器を製造して利用者に提供した後に、利用者機器を新たなコンテンツ供給システムに追加させるためには、例えば、ＩＣカードのような安全なデバイスを用いて利用者機器にノード鍵を追加するなど、特別な仕組み が必要となる。

【０３１１】また、第１の方法では、例えば。コンテンツ供給システムが任意の加入機器集合を１つにまとめて鍵を配布したい場合も、木構造が定まってしまっているため、ばらばらに配布する必要があり、暗号化鍵情報が増加し非効率である。

（ｂ）システム間の秘匿性の欠如（第１の方法の課題）

第１の方法では、コンテンツ供給システムのシステム管理者は、木のすべてのノード鍵を共有している。あるコンテンツ供給システムで用いるグループ鍵は、別のコンテンツ供給システムのシステム管理者に知られ得る。

【０３１２】（ｃ）機器の秘密に保持する鍵の容量が多い（第２の方法の課題）

第２の方法では、利用者機器はリーフからルートに至るノード鍵を、それぞれのコンテンツ供給システムの木構造に対応してすべて秘密に保存する必要がある。利用者機器が加入するコンテンツ供給システムが多ければ、利用者機器内の秘密の鍵保存用に大きなメモリが必要となる。

【０３１３】ところが、以上説明したように、本発明によれば、１個の利用者機器が複数のコンテンツ供給システムに接続される場合に、それぞれのコンテンツ供給システムが柔軟で独自の木構造を用いたグループ鍵管理方法を使用することが可能になる。具体的には、鍵管理装置は、コンテンツ供給システムのシステム管理装置に対して、一方向性関数を施したシステム用機器鍵だけを配布する。システム管理装置は、システム用機器鍵を用いて、鍵を管理し、公開簿を生成する。各利用者機器は木構造のリーフに対応する機器鍵だけを保持し、機器鍵と各コンテンツ供給システム用の公開簿を用いて、木構造の下から上に順次対応するノード鍵を求める。

【０３１４】また、本発明によると、不正に暴露された特定の端末だけを排除し、その他の端末ではコンテンツの再生等が可能でありながら、記録メディアに格納される暗号化されたデータを少なく抑えることができる。また、本発明によると、次の特徴を有する。

（ａ）コンテンツ供給システムごとに自由に木構造を構築することができる。また、コンテンツ供給システムの追加も可能である。

（ｂ）コンテンツ供給システムで用いる木構造に用いられるノード鍵とグループ鍵を、別のコンテンツ供給システムのシステム管理者が知ることは困難である。

（ｃ）機器は１つの固有機器鍵のみを保管すればよい。

【０３１５】以上説明したように、本発明は、鍵管理装置と複数のコンテンツ供給装置と１個以上の利用者機器とから構成されるデータ配信システムであって、各コンテンツ供給装置は、それぞれ暗号化コンテンツを供給し、各利用者機器は、暗号化コンテンツを復号して利用し、各利用者機器へ当該利用者機器に固有の機器鍵を出力し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第１システム用機器鍵を生成し、生成した前記第１システム用機器鍵を当該コンテンツ供給装置へ出力する鍵管理装置と、それぞれ、前記第１システム用機器鍵を受け取り、受け取った前記第１システム用機器鍵に基づいて、デジ

タル著作物であるコンテンツを暗号化して暗号化コンテンツを生成し、生成した前記暗号化コンテンツを利用者機器へ出力する複数のコンテンツ供給装置と、それぞれ、前記機器鍵を受け取り、前記暗号化コンテンツを受け取り、前記機器鍵及び前記コンテンツ供給装置に固有のシステム情報に基づいて前記一方向性関数を用いて前記利用者機器に固有の第２システム用機器鍵を生成し、生成した前記第２システム用機器鍵に基づいて、受け取った前記暗号化コンテンツを復号して復号コンテンツを生成する１個以上の利用者機器とから構成される。また、鍵管理装置と複数のコンテンツ供給装置と１個の利用者機器とから構成されるデータ配信システムにおいて、前記鍵管理装置は、前記利用者機器へ当該利用者機器に固有の機器鍵を供給し、各コンテンツ供給装置は、それぞれ暗号化コンテンツを供給し、前記利用者機器は、暗号化コンテンツを復号して利用し、前記利用者機器へ当該利用者機器に固有の機器鍵を出力する機器鍵出力手段と、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第１システム用機器鍵を生成し、生成した第１システム用機器鍵を前記コンテンツ供給装置へ出力するシステム用機器鍵生成手段とを備える。また、鍵管理装置と複数のコンテンツ供給装置と１個の利用者機器とから構成されるデータ配信システムにおける前記コンテンツ供給装置であって、前記鍵管理装置は、前記利用者機器へ当該利用者機器に固有の機器鍵を出力し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第１システム用機器鍵を生成し、生成した前記第１システム用機器鍵を当該コンテンツ供給装置へ出力し、デジタル著作物であるコンテンツを記憶している配信手段と、前記鍵管理装置から前記第１システム用機器鍵を取得する取得手段と、前記第１システム用機器鍵に基づいて、前記コンテンツを暗号化して暗号化コンテンツを生成する暗号手段と、生成した前記暗号化コンテンツを利用者機器へ出力する出力手段とを備える。また、鍵管理装置と複数のコンテンツ供給装置と１個の利用者機器とから構成されるデータ配信システムにおける前記利用者機器であって、前記鍵管理装置は、前記利用者機器へ当該利用者機器に固有の機器鍵を出力し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第１システム用機器鍵を生成し、生成した前記第１システム用機器鍵を当該コンテンツ供給装置へ出力し、各コンテンツ供給装置は、前記第１システム用機器鍵を受け取り、受け取った前記第１システム用機器鍵に基づいて、デジタル著作物であるコンテンツを暗号化して暗号化コンテンツを生成し、生成した前記暗号化コンテンツを利用者機器へ出力し、前記鍵管理装置から前記機器鍵を受け取る取得手段と、前記コンテンツ供給装置から前記暗号化コンテンツを受け取る受信手段と、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて前記一方向性関数を用いて前記利用者機器に固有の第２システム用機器鍵を生成するシステム用機器鍵生成手段と、生成した第２システム用機器鍵に基づいて、受け取った前記暗号化コンテンツを復号して復号コンテンツを生成する復号手段とを備える。

【０３１６】これらの構成によると、各コンテンツ供給装置は、柔軟で独自の鍵の管理を行うことができる。ここで、鍵管理装置と複数のコンテンツ供給装置と１個の利用者機器とから構成されるデータ配信システムであって、各コンテンツ供給装置は、それぞれ暗号化コンテンツを供給し、前記利用者機器は、暗号化コンテンツを復号して利用し、前記利用者機器へ当該利用者機器に固有の機器鍵を出力し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第１システム用機器鍵を生成し、生成した前記第１システム用機器鍵を当該コンテンツ供給装置へ出力するシステム用機器鍵生成手段とを備え、前記利用者機器は、前記第１システム用機器鍵を当該コンテンツ供給装置へ出力する鍵管理装置と、それぞれ、前記第１システム用機器鍵を受け取り、前記第１システム用機器鍵に基づいて、コンテンツを暗号化する際に基づくデバイス鍵を決定し、決定した前記デバイス鍵に基づいて、デジタル著作物であるコンテンツを暗号化して暗号化コンテンツを生成し、前記暗号化コンテンツを前記利用者機器へ出力し、前記第１システム用機器鍵に基づいて、前記デバイス鍵を特定するための公開情報を生成し、生成した前記公開情報を公開する複数のコンテンツ供給装置と、それぞれ、前記機器鍵を受け取り、前記暗号化コンテンツを受け取り、公開された前記公開情報を取得し、前記機器鍵及び前記コンテンツ供給装置に固有のシステム情報に基づいて前記一方向性関数を用いて前記利用者機器に固有の第２システム用機器鍵を生成し、前記第２システム用機器鍵に基づいて、前記公開情報から前記デバイス鍵を特定し、特定した前記デバイス鍵に基づいて、受け取った前記暗号化コンテンツを復号して復号コンテンツを生成する１個の利用者機器とから構成される。また、鍵管理装置と複数のコンテンツ供給装置と１個の利用者機器とから構成されるデータ配信システムにおける前記コンテンツ供給装置であって、前記鍵管理装置は、前記利用者機器へ当該利用者機器に固有の機器鍵を出力し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第１システム用機器鍵を生成し、生成した前記第１システム用機器鍵を当該コンテンツ供給装置へ出力し、デジタル著作物であるコンテンツを記憶している記憶手段と、前記鍵管理装置から前記第１システム用機器鍵を取得する取得手段と、前記第１

システム用機器鍵に基づいて、コンテンツを暗号化する際に基づくデバイス鍵を決定し、決定した前記デバイス鍵に基づいて、前記コンテンツを暗号化して暗号化コンテンツを生成する暗号手段と、前記第１システム用機器鍵に基づいて、前記デバイス鍵を特定するための公開簿を生成する公開簿生成手段と、生成した前記公開簿を公開し、生成した前記暗号化コンテンツを利用者機器へ出力する出力手段とを備える。また、鍵管理装置と複数のコンテンツ供給装置と１個の利用者機器とから構成されるデータ配信システムにおける前記利用者機器であって、前記鍵管理装置は、前記利用者機器へ当該利用者機器に固有の機器鍵を出力し、各コンテンツ供給装置については、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第１システム用機器鍵を生成し、生成した前記第１システム用機器鍵を当該コンテンツ供給装置へ出力し、各コンテンツ供給装置は、前記第１システム用機器鍵を受け取り、前記第１システム用機器鍵に基づいて、コンテンツを暗号化する際に基づくデバイス鍵を決定し、決定した前記デバイス鍵に基づいて、デジタル著作物であるコンテンツを暗号化して暗号化コンテンツを生成し、前記暗号化コンテンツを前記利用者機器へ出力し、前記第１システム用機器鍵に基づいて、前記デバイス鍵を特定するための公開簿を生成し、生成した前記公開簿を公開し、前記鍵管理装置から前記機器鍵を受け取り、公開された前記公開簿を取得し、前記コンテンツ供給装置から前記暗号化コンテンツを受け取る取得手段と、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて前記一方向性関数を用いて前記利用者機器に固有の第２システム用機器鍵を生成するシステム用機器鍵生成手段と、前記第２システム用機器鍵に基づいて、前記公開簿から前記デバイス鍵を特定するデバイス鍵特定手段と、特定した前記デバイス鍵に基づいて、受け取った前記暗号化コンテンツを復号して復号コンテンツを生成する復号手段とを備える。

【０３１７】これらの構成によると、利用者機器に割り当てられるデバイス鍵に基づいて、コンテンツが暗号化され、利用者機器は、公開される公開簿からデバイス鍵を取得でき、取得したデバイス鍵により暗号化コンテンツを復号できるので、当該利用者機器以外の機器により、暗号化コンテンツが不用意に復号されることがない。

【０３１８】また、前記コンテンツ供給装置は、前記第１システム用機器鍵がリーフに割り当てられ、他のノードにノード鍵が割り当てられた木構造を備え、前記木構造を用いて管理されている１個以上のノード鍵の中から前記デバイス鍵を決定し、前記デバイス鍵を用いて前記公開簿を生成し、前記利用者機器は、前記木構造を用いて、前記公開簿から、前記デバイス鍵を特定する。また、前記コンテンツ供給装置は、前記第１システム用機器鍵がリーフに割り当てられ、他のノードにノード鍵が割り当てられた木構造を備え、前記木構造を用いて管理されている１個以上のノード鍵の中から前記デバイス鍵を決定し、前記デバイス鍵特定手段は、前記木構造を用いて、前記公開簿から、前記デバイス鍵を特定する。また、前記暗号手段は、前記第１システム用機器鍵がリーフに割り当てられ、他のノードにノード鍵が割り当てられた木構造を備え、前記木構造を用いて管理されている１個以上のノード鍵の中から前記デバイス鍵を決定する。

【０３１９】これらの構成によると、木構造を用いて鍵を管理するので、コンテンツ供給装置が管理すべき鍵情報のデータ量を少なくすることができる。前記コンテンツ供給装置は、生成した前記公開簿を、Ｗｅｂサーバ、パッケージメディア又は放送メディアを介して、公開し、前記利用者機器は、Ｗｅｂサーバ、パッケージメディア又は放送メディアを介して、前記公開簿を取得する。また、前記出力手段は、生成した前記公開簿を、Ｗｅｂサーバ、パッケージメディア又は放送メディアを介して、公開する。また、前記コンテンツ供給装置は、生成した前記公開簿を、Ｗｅｂサーバ、パッケージメディア又は放送メディアを介して、公開し、前記取得手段は、Ｗｅｂサーバ、パッケージメディア又は放送メディアを介して、前記公開簿を取得する。

【０３２０】これらの構成によると、公開される暗号化鍵情報は、Ｗｅｂサーバ、パッケージメディア、又は放送メディアを介して利用者機器へ送信されるので、利用者機器は、いずれかのメディアを介して、容易に暗号化鍵情報を取得することができる。ここで、前記コンテンツ供給装置は、前記公開簿のうち、前記利用者機器に関連する情報のみを出力し、前記利用者機器は、前記公開簿のうち、前記利用者機器に関連する情報のみを取得する。また、前記公開簿生成手段は、前記公開簿のうち、前記利用者機器に関連する利用者機器関連情報のみを生成し、前記出力手段は、前記利用者機器関連情報を、公開する。また、前記コンテンツ供給装置は、前記公開簿のうち、前記利用者機器に関連する利用者機器関連情報のみを生成して公開し、前記取得手段は、前記利用者機器関連情報を取得し、前記デバイス鍵特定手段は、取得した前記利用者機器関連情報から当該利用者機器に対応する前記デバイス鍵を特定する。

【０３２１】これらの構成によると、暗号化鍵情報のうち、利用者機器に関連する情報のみが利用者機器に送信されるので、送信されるデータ量を少なく抑えることができる。ここで、前記公開簿生成手段は、前記木構造のリーフを除く各ノードについて、当該ノードに割り当てられたノード鍵を、当該ノードの子ノードに割り当てられたノード鍵を用いて暗号化して暗号化ノード鍵を生成し、生成した暗号化ノード鍵を含む前記公開簿を生成する。また、前記コンテンツ供給装置は、前記木構造のリ

ーフを除く各ノードについて、当該ノードに割り当てられたノード鍵を、当該ノードの子ノードに割り当てられたノード鍵を用いて暗号化して暗号化ノード鍵を生成し、生成した暗号化ノード鍵を含む前記公開簿を生成し、前記デバイス鍵特定手段は、前記木構造の１個のノードに対応するノード鍵を用いて、取得した前記公開簿内の暗号化ノード鍵を復号して、当該ノードの親ノードのノード鍵を求める。

【０３２２】これらの構成によると、子ノード鍵で親ノード鍵を暗号化し、暗号化親ノード鍵を復号して子ノード鍵を求めることができるので、木構造の子ノードから親ノードの方向へ向かって、ノード鍵を求めることができる。ここで、前記公開簿生成手段は、前記木構造のリーフを除く各ノードについて、（ａ）当該ノードの１個の子ノードに割り当てられたノード鍵に一方向性関数を施して、当該ノードのノード鍵を生成し、（ｂ）当該ノードの別の子ノードに割り当てられたノード鍵を用いて、生成した当該ノードのノード鍵を暗号化して暗号化ノード鍵を生成し、（ｃ）生成した暗号化ノード鍵を含む前記公開簿を生成する。また、前記コンテンツ供給装置は、前記木構造のリーフを除く各ノードについて、（ａ）当該ノードの１個の子ノードに割り当てられたノード鍵に一方向性関数を施して、当該ノードのノード鍵を生成し、（ｂ）当該ノードの別の子ノードに割り当てられたノード鍵を用いて、生成した当該ノードのノード鍵を暗号化して暗号化ノード鍵を生成し、（ｃ）生成した暗号化ノード鍵を含む前記公開簿を生成し、前記デバイス鍵特定手段は、前記木構造の１個のノードに対応するノード鍵を用いて公開された公開簿内の暗号化ノード鍵を復号した復号文、又は当該ノードに対応するノード鍵に一方向性関数を施して得られた出力値を選択し、選択した値を当該ノードの親ノードのノード鍵として求める。

【０３２３】これらの構成によると、親ノード鍵の生成の一部において、子ノード鍵に一方向性関数を施して親ノード鍵を生成するので、公開される暗号化鍵情報のデータ量を少なく抑えることができる。ここで、ｋを２以上の整数とし、ｍを０以上の整数とし、前記木構造をｋ分木とし、各ノード鍵を（ｘ，ｙ）平面上の点とみなし、前記公開簿生成手段は、（ｘ，ｙ）平面上において、共通の親ノードを持つｋ個の全てのノードのノード鍵を結ぶ（ｋ＋ｍ－１）次の曲線を生成し、前記曲線上のノード鍵以外の（ｋ＋ｍ－１）個の点を含む前記公開簿を生成する。また、ｋを２以上の整数とし、ｍを０以上の整数とし、前記木構造をｋ分木とし、各ノード鍵を（ｘ，ｙ）平面上の点とみなし、前記コンテンツ供給装置は、（ｘ，ｙ）平面上において、共通の親ノードを持つｋ個の全てのノードのノード鍵を結ぶ（ｋ＋ｍ－１）次の曲線を生成し、前記曲線上のノード鍵以外の（ｋ＋ｍ－１）個の点を含む前記公開簿を生成し、前記デバイス鍵特定手段は、前記木構造の１個のノードに対応するノード鍵と、公開された公開簿内の（ｋ＋ｍ－１）個の点とを結ぶ、（ｋ＋ｍ－１）次の曲線を求め、さらにこの曲線から一方向性関数を用いて当該ノードの親ノードに対応するノード鍵を求める。

【０３２４】これらの構成によると、安全性を保ちつつ、確実にノード鍵を復号できる。ここで、前記公開簿生成手段は、（ａ）公開鍵暗号の秘密鍵と公開鍵のペアを生成し、（ｂ）生成した前記秘密鍵を秘密に保持し、生成した前記公開鍵を含む前記公開簿を生成し、（ｃ）前記木構造のリーフを除く各ノードについて、当該ノードに対応するノード鍵に基づいて、前記秘密鍵を用いて暗号化して暗号化ノード鍵を生成し、生成した暗号化ノード鍵を、当該ノードの子ノードに対応するノード鍵とし、前記出力手段は、前記公開簿を公開する。また、前記コンテンツ供給装置は、（ａ）公開鍵暗号の秘密鍵と公開鍵のペアを生成し、（ｂ）生成した前記秘密鍵を秘密に保持し、生成した前記公開鍵を含む前記公開簿を生成し、（ｃ）前記木構造のリーフを除く各ノードについて、当該ノードに対応するノード鍵に基づいて、前記秘密鍵を用いて暗号化して暗号化ノード鍵を生成し、生成した暗号化ノード鍵を、当該ノードの子ノードに対応するノード鍵とし、（ｄ）前記公開簿を公開し、前記デバイス鍵特定手段は、前記木構造の１個のノードに対応するノード鍵を、公開された公開簿内の公開鍵を用いて復号し、その結果を当該ノードの親ノードに対応するノード鍵とする。

【０３２５】これらの構成によると、公開鍵暗号方式を用いるので、安全性を保ちつつ、確実にノード鍵を復号できる。

【図面の簡単な説明】

【図１】暗号化データ配信システム１の構成を示すブロック図である。

【図２】鍵管理装置１００の構成を示すブロック図である。

【図３】機器鍵管理テーブル１１１のデータ構造を示す。

【図４】システム用機器鍵管理テーブル１２１のデータ構造を示す。

【図５】音楽配信システム管理装置２００の構成を示すブロック図である。

【図６】木構造Ｔ１００を示す概念図である。

【図７】音楽配信用木構造テーブル２１１のデータ構造を示す。

【図８】音楽用公開簿２２１のデータ構造を示す。

【図９】公開簿サーバ装置４００の構造を示すブロック図である。

【図１０】音楽コンテンツ配信装置３００の構造を示すブロック図である。

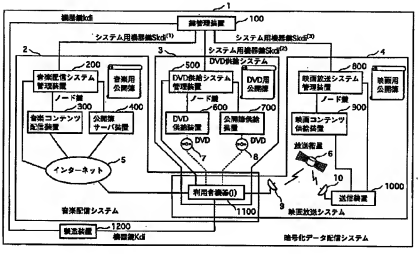
【図１１】ＤＶＤ供給システム管理装置５００の構造を

示すブロック図である。
【図１２】ＤＶＤ用木構造テーブル５１１のデータ構造を示す。
【図１３】木構造Ｔ２００を示す概念図である。
【図１４】ＤＶＤ用公開簿５２１のデータ構造を示す。
【図１５】映画放送システム管理装置８００の構造を示すブロック図である。
【図１６】木構造Ｔ３００を示す概念図である。
【図１７】映画放送用木構造テーブル８１１のデータ構造を示す。
【図１８】公開簿生成部８０６による公開簿生成の手順を示すｘ－ｙ座標空間上の概念図である。
【図１９】木構造Ｔ３００の一部分を示す概念図である。
【図２０】映画用公開簿８２１のデータ構造を示す。
【図２１】利用者機器１１００の構造を示すブロック図である。
【図２２】鍵管理装置１００の動作を示すフローチャートである。
【図２３】音楽配信システム管理装置２００の動作を示すフローチャートである。
【図２４】公開簿生成部２０６による音楽用公開簿の生成の動作を示すフローチャートである。図２５へ続く。
【図２５】公開簿生成部２０６による音楽用公開簿の生成の動作を示すフローチャートである。図２４から続く。
【図２６】音楽コンテンツ配信装置３００の動作を示すフローチャートである。
【図２７】ＤＶＤ供給システム管理装置５００の全体の動作を示すフローチャートである。
【図２８】ノード鍵生成部５０５によるノード鍵の生成の動作を示すフローチャートである。
【図２９】公開簿生成部５０６によるＤＶＤ用公開簿の生成の動作を示すフローチャートである。図３０へ続く。
【図３０】公開簿生成部５０６によるＤＶＤ用公開簿の生成の動作を示すフローチャートである。図２９から続く。
【図３１】映画放送システム管理装置８００の動作を示すフローチャートである。図３２へ続く。
【図３２】映画放送システム管理装置８００の動作を示すフローチャートである。図３３へ続く。
【図３３】映画放送システム管理装置８００の動作を示すフローチャートである。図３２から続く。
【図３４】利用者機器１１００全体の動作を示すフローチャートである。
【図３５】ノード鍵特定部１１０３によるノード鍵の特定（１）の動作を示すフローチャートである。図３６へ続く。
【図３６】ノード鍵特定部１１０３によるノード鍵の特定（１）の動作を示すフローチャートである。図３５から続く。
【図３７】ノード鍵特定部１１０３によるノード鍵の特定（２）の動作を示すフローチャートである。図３８へ続く。
【図３８】ノード鍵特定部１１０３によるノード鍵の特定（２）の動作を示すフローチャートである。図３９へ続く。
【図３９】ノード鍵特定部１１０３によるノード鍵の特定（２）の動作を示すフローチャートである。図４０へ続く。
【図４０】ノード鍵特定部１１０３によるノード鍵の特定（２）の動作を示すフローチャートである。図３９から続く。
【図４１】ノード鍵特定部１１０３によるノード鍵の特定（３）の動作を示すフローチャートである。図４２へ続く。
【図４２】ノード鍵特定部１１０３によるノード鍵の特定（３）の動作を示すフローチャートである。図４３へ続く。
【図４３】ノード鍵特定部１１０３によるノード鍵の特定（３）の動作を示すフローチャートである。図４２から続く。
【図４４】木構造Ｔ４００を示す概念図である。
【図４５】音楽配信用木構造テーブル２１１ｂのデータ構造を示す。
【図４６】音楽用公開簿２２１ｂのデータ構造を示す。
【図４７】音楽配信システム管理装置２００ｂの動作を示すフローチャートである。図４８へ続く。
【図４８】音楽配信システム管理装置２００ｂの動作を示すフローチャートである。図４９へ続く。
【図４９】音楽配信システム管理装置２００ｂの動作を示すフローチャートである。図５０へ続く。
【図５０】音楽配信システム管理装置２００ｂの動作を示すフローチャートである。図５１へ続く。
【図５１】音楽配信システム管理装置２００ｂの動作を示すフローチャートである。図５０から続く。
【図５２】利用者機器１１００ｂの動作のうち、ノード鍵特定部１１０３ｂによるノード鍵の特定（１）の動作を示すフローチャートである。図５３へ続く。
【図５３】利用者機器１１００ｂの動作のうち、ノード鍵特定部１１０３ｂによるノード鍵の特定（１）の動作を示すフローチャートである。図５２から続く。
【図５４】非特許文献１により開示されている木構造分割方法における木構造を示す概念図である。
【符号の説明】
１　暗号化データ配信システム
２　音楽配信システム
３　ＤＶＤ供給システム
４　映画放送システム

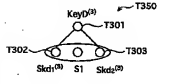
１００	鍵管理装置
２００	音楽配信システム管理装置
３００	音楽コンテンツ配信装置
４００	公開簿サーバ装置
５００	ＤＶＤ供給システム管理装置
６００	ＤＶＤ供給装置

＊７００	公開簿供給装置
８００	映画放送システム管理装置
９００	映画コンテンツ供給装置
１０００	送信装置
１１００	利用者機器
＊　１２００	製造装置

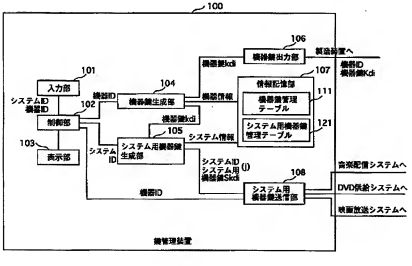
【図１】



【図１９】



【図２】



【図３】

機器鍵管理テーブル　111

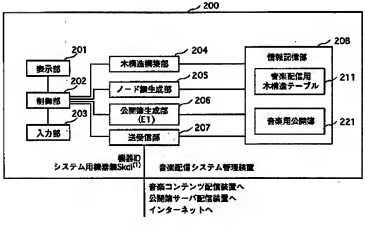
機器情報	
機器ID	機器鍵Kdi
1001	Kdn
1002	Kde
1003	Kda
⋮	⋮

【図４】

システム用機器鍵管理テーブル　121

システム情報		
機器ID	システムID (j)	システム用機器鍵Skdi(j)
1001	1	$Skdn^{(1)}$
1002	1	$Skde^{(1)}$
1003	1	$Skda^{(1)}$
⋮	⋮	⋮
1001	2	$Skdn^{(2)}$
1002	2	$Skde^{(2)}$
1003	2	$Skda^{(2)}$
⋮	⋮	⋮

【図５】



【図７】

音楽配信用木構造テーブル　211

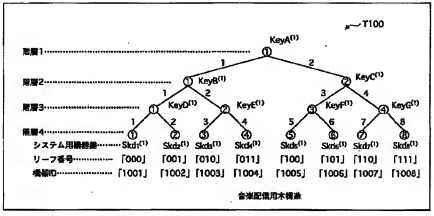
ノード情報			
階層番号	ノード番号	ノード鍵	機器ID
1	1	$KeyA^{(j)}$	—
2	1	$KeyB^{(j)}$	—
2	2	$KeyC^{(j)}$	—
3	1	$KeyD^{(j)}$	—
3	2	$KeyE^{(j)}$	—
3	3	$KeyF^{(j)}$	—
3	4	$KeyG^{(j)}$	—
4	1	$Skdn^{(j)}$	1001
4	2	$Skda^{(j)}$	1002
4	3	$Skdn^{(j)}$	1003
4	4	$Skda^{(j)}$	1004
4	5	$Skda^{(j)}$	1005
4	6	$Skde^{(j)}$	1006
4	7	$Skdn^{(j)}$	1007
4	8	$Skda^{(j)}$	1008

【図１４】

DVD用公開鍵　S21

システムID	2
公開情報	
インデックス情報（階層番号,ノード番号）	暗号化ノード鍵
(3, 1)	$E4(Skda^{(2)},KeyD^{(2)})$
(3, 2)	$E4(Skdn^{(2)},KeyE^{(2)})$
(3, 3)	$E4(Skda^{(2)},KeyE^{(2)})$
(3, 4)	$E4(Skdn^{(2)},KeyG^{(2)})$
(2, 1)	$E4(KeyE^{(2)},KeyB^{(2)})$
(2, 2)	$E4(KeyG^{(2)},KeyC^{(2)})$
(1, 1)	$E4(KeyC^{(2)},KeyA^{(2)})$

【図６】

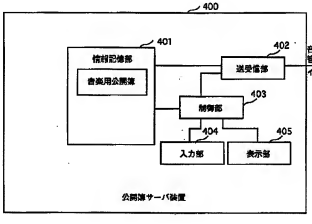


【図８】

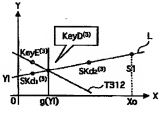
音楽用公開鍵 221

システムID	1
公開情報	
インデックス情報（階層番号、パス番号）	暗号化ノード鍵
(3, 1)	E1(Skd1(1),KeyD(1))
(3, 2)	E1(Skd2(1),KeyD(1))
(3, 3)	E1(Skd3(1),KeyE(1))
(3, 4)	E1(Skd4(1),KeyE(1))
(3, 5)	E1(Skd5(1),KeyF(1))
(3, 6)	E1(Skd6(1),KeyF(1))
(3, 7)	E1(Skd7(1),KeyG(1))
(3, 8)	E1(Skd8(1),KeyG(1))
(2, 1)	E1(KeyD(1),KeyB(1))
(2, 2)	E1(KeyE(1),KeyB(1))
(2, 3)	E1(KeyE(1),KeyC(1))
(2, 4)	E1(KeyG(1),KeyC(1))
(1, 1)	E1(KeyB(1),KeyA(1))
(1, 2)	E1(KeyC(1),KeyA(1))

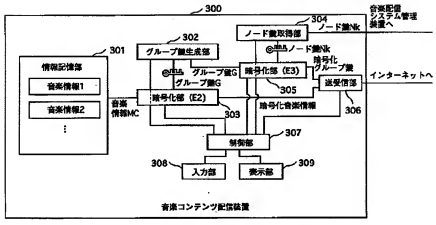
【図９】



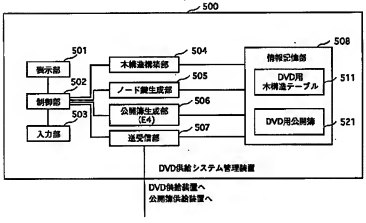
【図１８】



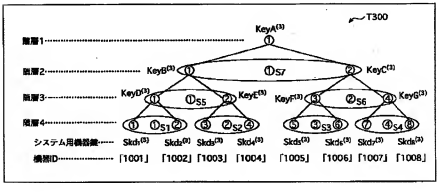
【図１０】


300
音楽配信システム管理装置へ
ノード鍵取得部
304
ノード鍵
302
グループ鍵生成部
ノード鍵
301
情報記憶部
音楽情報1
音楽情報2
グループ鍵G
暗号化部（E3）
暗号化グループ鍵
インターネットへ
送受信部
暗号化部（E2）
305
音楽情報MC
暗号化音楽情報
306
303
307
制御部
308
入力部
表示部
309
音楽コンテンツ配信装置

【図１１】


500
501
表示部
502
制御部
503
入力部
木構造構築部
504
ノード鍵生成部
505
公開鍵生成部（E4）
506
送受信部
507
508
情報記憶部
DVD用木構造テーブル
511
DVD用公開鍵
521
DVD供給システム管理装置
DVD供給装置へ
公開鍵供給装置へ

【図１６】


T300
階層1
階層2
階層3
階層4
システム用機器鍵
機器ID
「1001」「1002」「1003」「1004」「1005」「1006」「1007」「1008」

【図１２】

DVD用木構造テーブル　511

ノード情報			
階層番号	ノード番号	ノード鍵	機器ID
1	1	$Key_A^{(2)}=g(Key_B^{(2)})$	—
2	1	$Key_B^{(2)}=g(Key_D^{(2)})$	—
2	2	$Key_C^{(2)}=g(Key_E^{(2)})$	—
3	1	$Key_D^{(2)}=g(Skd_1^{(2)})$	—
3	2	$Key_E^{(2)}=g(Skd_2^{(2)})$	—
3	3	$Key_F^{(2)}=g(Skd_3^{(2)})$	—
3	4	$Key_G^{(2)}=g(Skd_4^{(2)})$	—
4	1	$Skd_1^{(2)}$	1001
4	2	$Skd_2^{(2)}$	1002
4	3	$Skd_3^{(2)}$	1003
4	4	$Skd_4^{(2)}$	1004
4	5	$Skd_5^{(2)}$	1005
4	6	$Skd_6^{(2)}$	1006
4	7	$Skd_7^{(2)}$	1007
4	8	$Skd_8^{(2)}$	1008

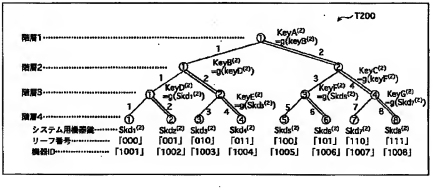
【図１７】

映画放送用木構造テーブル　811

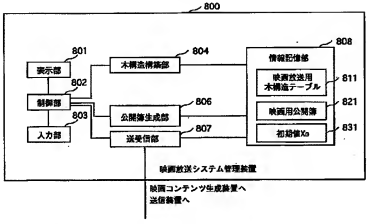
ノード情報			
階層番号	ノード番号	ノード鍵	機器ID
1	1	$Key_A^{(3)}$	—
2	1	$Key_B^{(3)}$	—
2	2	$Key_C^{(3)}$	—
3	1	$Key_D^{(3)}$	—
3	2	$Key_E^{(3)}$	—
3	3	$Key_F^{(3)}$	—
3	4	$Key_G^{(3)}$	—
4	1	$Skd_1^{(3)}$	1001
4	2	$Skd_2^{(3)}$	1002
4	3	$Skd_3^{(3)}$	1003
4	4	$Skd_4^{(3)}$	1004
4	5	$Skd_5^{(3)}$	1005
4	6	$Skd_6^{(3)}$	1006
4	7	$Skd_7^{(3)}$	1007
4	8	$Skd_8^{(3)}$	1008

812
813

【図１３】



【図１５】

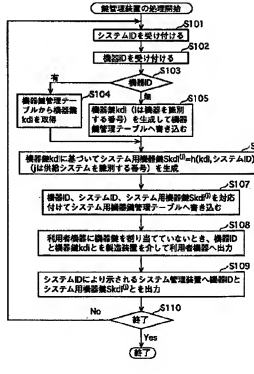


【図２０】

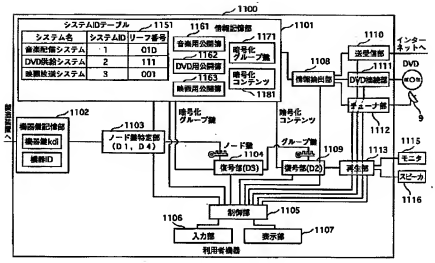
映画用公開鍵 821

システムID	3
公開情報	
初期値	X_0
インデックス情報（階層番号、公開点のノード番号）	公開点Y_i値等
(4, 1)	$S1_{(Y)}$
(4, 2)	$S2_{(Y)}$
(4, 3)	$S3_{(Y)}$
(4, 4)	$S4_{(Y)}$
(3, 1)	$S5_{(Y)}$
(3, 2)	$S6_{(Y)}$
(2, 1)	$S7_{(Y)}$

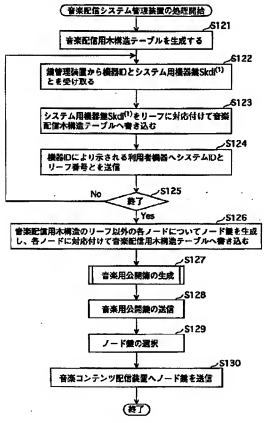
【図２２】



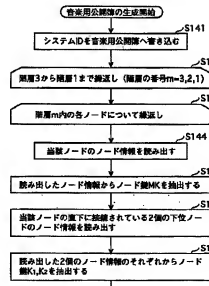
【図２１】


1100
システムIDテーブル
1151
1161
情報記憶部
1101
システム名
システムID
リーフ番号
音楽配信システム
1
010
DVD再録システム
2
111
映画放送システム
3
001
音楽用公開鍵
1171
暗号化グループ鍵
1162
DVD用公開鍵
暗号化コンテンツ
1163
映画用公開鍵
1181
1108
情報抽出部
1110
送受信部
インターネットへ
1111
DVD機能部
DVD
ON
ダミー部
9
1112
1102
機器個別情報
機器鍵kd
機器ID
1103
ノード鍵物定部
(D1，D4)
暗号化グループ鍵
暗号化コンテンツ
1104
ノード鍵
グループ鍵
1109
1113
1115
モニタ
復号部(D3)
復号部(D2)
再生部
スピーカ
1116
制御部
1105
1106
入力部
1107
表示部
利用者機器
機器固有

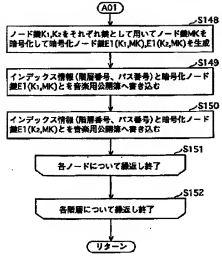
【図２３】


音楽配信システム管理装置の処理開始
S121
音楽配信用木構造テーブルを生成する
S122
鍵管理装置から機器IDとシステム用機器鍵Skd(1)とを受け取る
S123
システム用機器鍵Skd(1)をリーフに対応付けて音楽配信木構造テーブルへ書き込む
S124
機器IDにより示される利用者機器へシステムIDとリーフ番号とを送信
S125
終了
No
Yes
S126
音楽配信用木構造のリーフ以外の各ノードについてノード鍵を生成し、各ノードに対応付けて音楽配信木構造テーブルへ書き込む
S127
音楽用公開鍵の生成
S128
音楽用公開鍵の送信
S129
ノード鍵の選択
S130
音楽コンテンツ配信装置へノード鍵を送信
終了

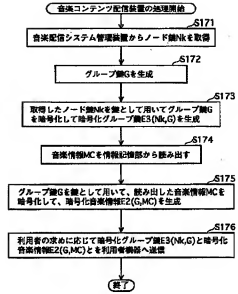
【図２４】


音楽用公開鍵の生成開始
S141
システムIDを音楽用公開鍵へ書き込む
S142
第層3から第層1まで繰返し（第層の番号m=3,2,1）
S143
第層m内の各ノードについて繰返し
S144
当該ノードのノード情報を読み出す
S145
読み出したノード情報からノード鍵MKを抽出する
S146
当該ノードの直下に接続されている2個の下位ノードのノード情報を読み出す
S147
読み出した2個のノード情報のそれぞれからノード鍵K1,K2を抽出する
A01

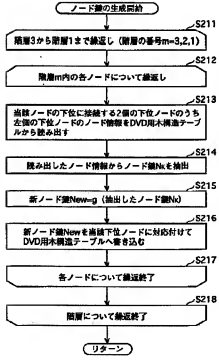
【図２５】



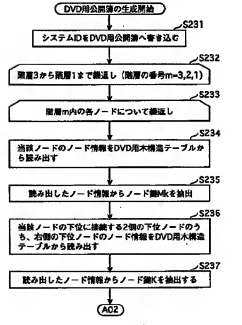
【図２６】



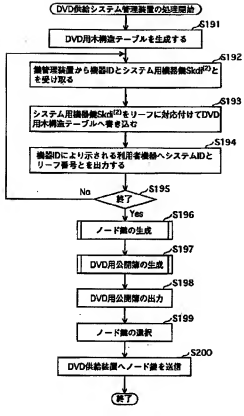
【図２８】



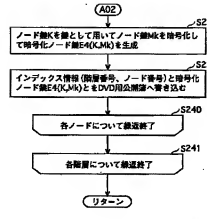
【図２９】



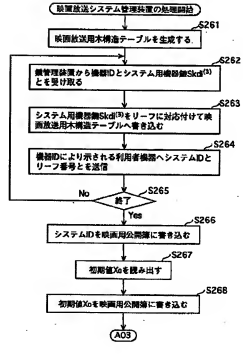
【図２７】



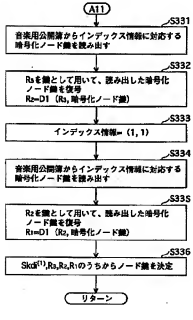
【図３０】



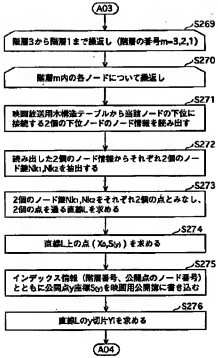
【図３１】



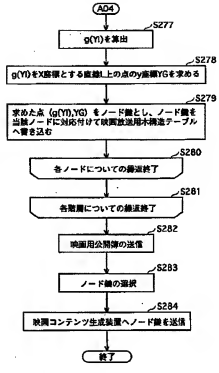
【図３６】



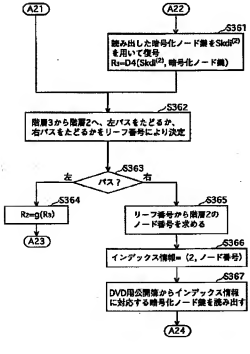
【図３２】



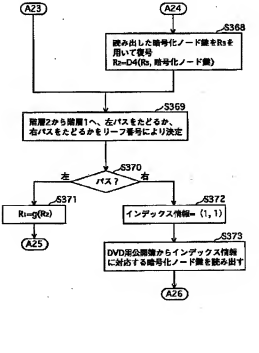
【図３３】



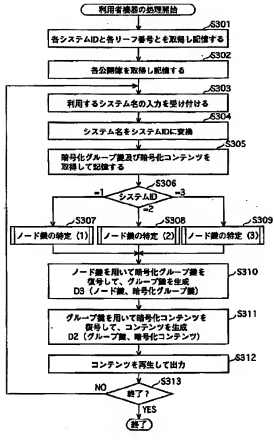
【図３８】



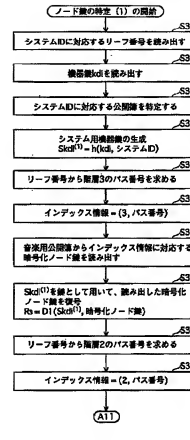
【図３９】



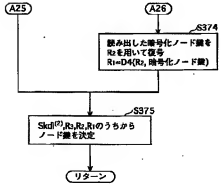
【図３４】



【図３５】



【図４０】

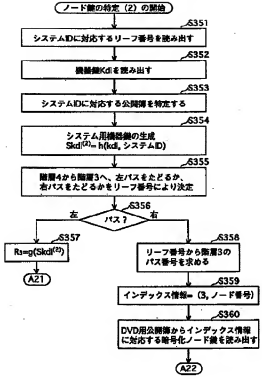


【図４５】

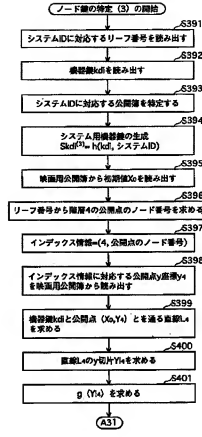
音楽配信用木構造テーブル　211b

ノード情報				
階層番号	ノード番号	ノード鍵	機器ID	パス情報
1	1	$KeyA^{(1)}$	—	—
2	1	$KeyB^{(1)}$	—	P_1
2	2	$KeyC^{(1)}$	—	P_2
3	1	$KeyD^{(1)}$	—	P_3
3	2	$KeyE^{(1)}$	—	P_4
3	3	$KeyF^{(1)}$	—	P_5
3	4	$KeyG^{(1)}$	—	P_6
4	1	$Skdi^{(1)}$	1001	—
4	2	$Skdi^{(1)}$	1002	—
4	3	$Skdi^{(1)}$	1003	—
4	4	$Skdi^{(1)}$	1004	—
4	5	$Skdi^{(1)}$	1005	—
4	6	$Skdi^{(1)}$	1006	—
4	7	$Skdi^{(1)}$	1007	—
4	8	$Skdi^{(1)}$	1008	—

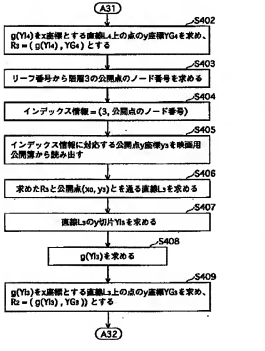
【図３７】



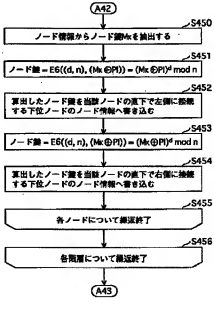
【図４１】



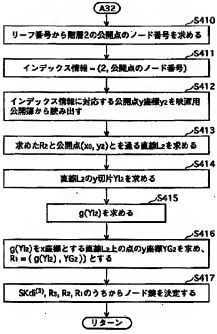
【図４２】



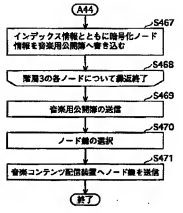
【図４９】



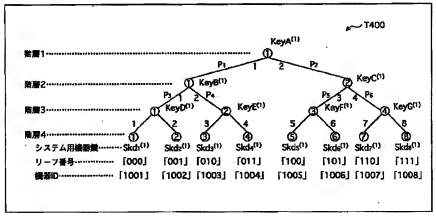
【図４３】


A32
S410
リーフ番号から階層2の公開点のノード番号を求める
S411
インデックス情報 = (2, 公開点のノード番号)
S412
インデックス情報に対応するy座標yzを映画用公開部から読み出す
S413
求めたRzと公開点(x0, yz)とを通る直線Lzを求める
S414
直線Lzのy切片Yizを求める
S415
g(Yiz)を求める
S416
g(Yiz)をx座標とする直線L上の点のy座標YGzを求め、Ri = (g(Yiz) , YGz))とする
S417
SKdi(3), Rs, Rz, Riのうちからノード鍵を決定する
リターン

【図５１】


A44
S467
インデックス情報とともに暗号化ノード情報を音楽用公開部へ書き込む
S468
階層3の各ノードについて繰返終了
S469
音楽用公開部の送信
S470
ノード鍵の選択
S471
音楽コンテンツ配信装置へノード鍵を送信
終了

【図４４】

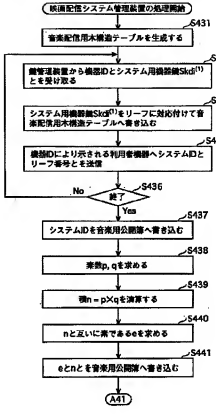

T400
KeyA(1)
階層1
Ps 1 2 Ps
KeyB(1)
KeyC(1)
階層2
Ps 1 2 Ps
Ps 3 4 Ps
KeyD(1)
KeyE(1)
KeyE(1)
KeyG(1)
階層3
1 2 3 4 5 6 7 8
階層4
システム用機器鍵 Skdi(1) Skdi(1) Skdi(1) Skdi(1) Skdi(1) Skdi(1) Skdi(1) Skdi(1)
リーフ番号 「000」 「001」 「010」 「011」 「100」 「101」 「110」 「111」
機器ID 「1001」 「1002」 「1003」 「1004」 「1005」 「1006」 「1007」 「1008」

【図４６】

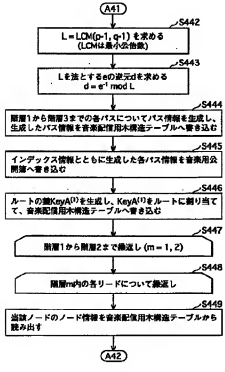
音楽用公開鍵　221b

システムID	1
パス公開情報	
公開鍵	e、n
インデックス情報（階層番号、パス番号）	パス情報
(1，1)	P1
(1，2)	P2
(2，1)	P3
(2，2)	P4
(2，3)	P5
(2，4)	P6
ノード鍵公開情報	
インデックス情報（階層番号、パス番号）	暗号化ノード鍵
(3，1)	E1 ($Skd_1^{(1)}$, $KeyD^{(1)}$)
(3，2)	E1 ($Skd_2^{(1)}$, $KeyD^{(1)}$)
(3，3)	E1 ($Skd_3^{(1)}$, $KeyE^{(1)}$)
(3，4)	E1 ($Skd_4^{(1)}$, $KeyE^{(1)}$)
(3，5)	E1 ($Skd_5^{(1)}$, $KeyF^{(1)}$)
(3，6)	E1 ($Skd_6^{(1)}$, $KeyF^{(1)}$)
(3，7)	E1 ($Skd_7^{(1)}$, $KeyG^{(1)}$)
(3，8)	E1 ($Skd_8^{(1)}$, $KeyG^{(1)}$)

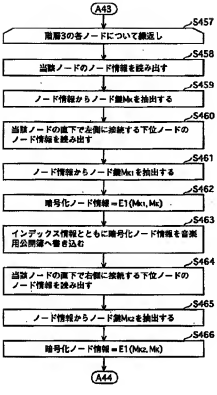
【図４７】



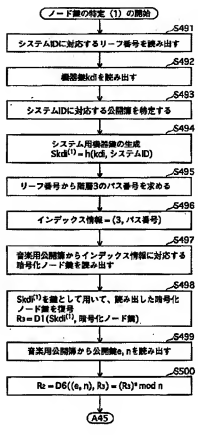
【図４８】



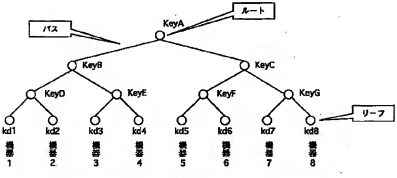
【図５０】


A43
S457
階層3の各ノードについて繰返し
S458
当該ノードのノード情報を読み出す
S459
ノード情報からノード鍵Mkを抽出する
S460
当該ノードの直下で左側に接続する下位ノードのノード情報を読み出す
S461
ノード情報からノード鍵Mk1を抽出する
S462
暗号化ノード情報＝E1(Mk1, Mk)
S463
インデックス情報とともに暗号化ノード情報を音楽用公開鍵へ書き込む
S464
当該ノードの直下で右側に接続する下位ノードのノード情報を読み出す
S465
ノード情報からノード鍵Mk2を抽出する
S466
暗号化ノード情報＝E1(Mk2, Mk)
A44

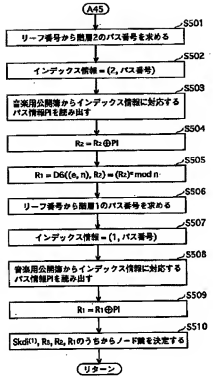
【図５２】


ノード鍵の特定（1）の開始
S491
システムIDに対応するリーフ番号を読み出す
S492
機器鍵kdiを読み出す
S493
システムIDに対応する公開鍵を特定する
S494
システム用機器鍵の生成
Skdi(1) = h(kdi, システムID)
S495
リーフ番号から階層3のパス番号を求める
S496
インデックス情報＝(3, パス番号)
S497
音楽用公開鍵からインデックス情報に対応する暗号化ノード鍵を読み出す
S498
Skdi(1)を鍵として用いて、読み出した暗号化ノード鍵を復号
R3＝D1(Skdi(1), 暗号化ノード鍵)
S499
音楽用公開鍵から公開鍵e, nを読み出す
S500
Re＝D6((e, n), R3)＝(R3)^e mod n
A45

【図５４】


パス
ルート
KeyA
KeyB
KeyC
KeyD
KeyE
KeyF
KeyG
リーフ
kd1
kd2
kd3
kd4
kd5
kd6
kd7
kd8
機器1
機器2
機器3
機器4
機器5
機器6
機器7
機器8

【図５３】



フロントページの続き

(72)発明者　松本　勉
横浜市青葉区柿の木台13－45

Ｆターム(参考)　5J104 AA12 AA16 EA01 EA04 EA15
EA19 EA32 JA03 JA21 JA28
JA31 MA05 NA02 NA11 NA12
NA18 PA01 PA05 PA14